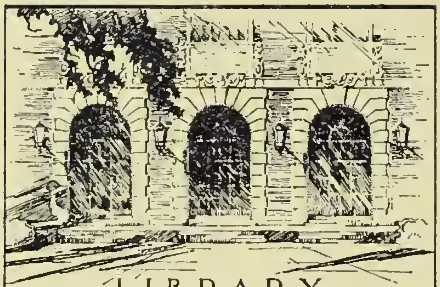


[redacted]

DIGITAL COMPUTER LABORATORY

UNIVERSITY OF ILLINOIS

URBANA, ILLINOIS

REPORT NO. 163

GENERAL THEORY OF MOST EFFICIENT CODES

by

Yasuo Komamiya

June 9, 1964

ACKNOWLEDGMENT

The author wishes to thank Professor David E. Muller for a number of helpful discussions in connection with this report, and Mrs. Phyllis Olson for her skillful typing of this paper.

TABLE OF CONTENTS

1. INTRODUCTION

In this paper, the number of most efficient binary codes and the construction methods are discussed in general, where the most efficient binary codes mean codes with a minimum Hamming distance of p.

The most efficient binary codes are defined mathematically as follows:

$$M(n,p) = \begin{pmatrix} x_{11}, & x_{12}, & x_{13}, & \dots, & x_{1n} \\ x_{21}, & x_{22}, & x_{23}, & \dots, & x_{2n} \\ x_{31}, & x_{32}, & x_{33}, & \dots, & x_{3n} \\ \vdots & & & & \\ x_{m1}, & x_{m2}, & x_{m3}, & \dots, & x_{mn} \end{pmatrix} \qquad (1.1)$$

Consider the matrix M(n,p), where $(x_{i1}, x_{i2}, \dots, x_{in})$ for $1 \leq i \leq m$ is an n digit binary code. Accordingly, x_{ij} is 1 or 0 and m is the number of most efficient binary codes. Here

$$|x_{i1} - x_{j1}| + |x_{i2} - x_{j2}| + \dots + |x_{in} - x_{jn}| \geq p \qquad \text{for any } i \neq j;\ 1 \leq i,\ j \leq m$$

where p is the minimum Hamming distance.

The purpose of this paper is to obtain maximum m and the value of each x_{ij}.

In Section 2, a theorem which plays an important role in the coding problem is discussed.

In Section 3, the matrix H(n,p) (by which the coding problem can be discussed in general) is introduced, and general theory discussed. As a result, the coding problem is reduced to the problem of determining the independence of some vectors.

In Section 4, the characteristic values of H(n,p) are discussed.

In Sections 5 and 6, some properties of the independence of vectors are discussed.

In Section 7, solution under some conditions (group code condition implies these conditions; accordingly, group code is a special case of these conditions) is discussed.

In Section 8, one method of general solution is discussed.

In Section 9, Boolean algebra is used in finding a general solution.

The c onclusion is stated in Section 10.

2. A THEOREM WHICH PLAYS AN IMPORTANT ROLE IN THE CODING PROBLEM

In this section a theorem which plays an important role in the coding problem is first described, followed by a discussion of a second, related theorem.

Definition 2.1. Exclusive-OR operation "$\oplus$" between any non-negative integers.

Let a, b be non-negative integers. Define $a \oplus b$ as follows: when a and b are expanded to binary form, i.e.,

$$a = a_n 2^n + a_{n-1} 2^{n-1} + \dots + a_1 2 + a_0$$

$$b = b_n 2^n + b_{n-1} 2^{n-1} + \dots + b_1 2 + b_0 \,,$$

$$a \oplus b = (a_n \oplus b_n) 2^n + (a_{n-1} \oplus b_{n-1}) 2^{n-1} + \dots + (a_1 \oplus b_1) 2 + (a_0 \oplus b_0) \,.$$

Here the symbol "$\oplus$" of the right-hand side of the above formula is an exclusive-or operation in the usual meaning.

Theorem 2.1. Let $z_0, z_1, \dots, z_{n-1}$ be real numbers. Consider the matrix

$$Z_n = \begin{pmatrix} z_0, & z_1, & z_2, & \dots, & z_{N-1} \\ z_1, & z_0, & z_3, & \dots, & z_{1\oplus(N-1)} \\ \vdots & & & & \\ z_i, & z_{i\oplus 1}, & z_{i\oplus 2}, & \dots, & z_{i\oplus(N-1)} \\ \vdots & & & & \\ z_{N-1}, & z_{N-2}, & z_{N-3}, & \dots, & z_0 \end{pmatrix}$$

where $N = 2^n$ and $n \geq 1$.

The matrix Z_n can be transformed to the diagonal matrix by the orthogonal matrix as follows:

$$Z_n = U_n \Lambda U_n$$

where

$$U_n = \frac{1}{\sqrt{N}} \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \cdots \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \equiv (u_0, u_1, \ldots, u_{(N-1)})$$

and

$$\Lambda = \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ 0 & & \ddots & \\ & & & x_{(N-1)} \end{pmatrix}$$

Here, the symbol "×" means the direct product (Kronecker's product) and

$$\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \cdots \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}$$

means the n direct products of $\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}$.

The following relations can also be obtained:

$$x_i = \sqrt{N}\ (z_0, z_1, \ldots, z_{(N-1)}) u_i$$

$$z_i = \frac{1}{\sqrt{N}}\ (x_0, x_1, \ldots, x_{(N-1)}) u_i$$

for any i, where $0 \leq i \leq (N - 1)$.

Proof. Since the matrix Z_n is a symmetric real matrix, Z_n can be transformed to a diagonal matrix by an orthogonal matrix. When n = 1, Z_1, U_1 are

$$Z_1 = \begin{pmatrix} z_0, & z_1 \\ z_1, & z_0 \end{pmatrix}$$

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} = (u_0, u_1)$$

respectively. The relation

$$U_1 \begin{pmatrix} x_0 & 0 \\ 0 & x_1 \end{pmatrix} U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \begin{pmatrix} x_0 & 0 \\ 0 & x_1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} x_0 + x_1, & x_0 - x_1 \\ x_0 - x_1, & x_0 + x_1 \end{pmatrix}$$

holds. Therefore, letting

$$z_0 = \frac{1}{2} (x_0 + x_1) = \frac{1}{2} (x_0, x_1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (x_0, x_1) u_0$$

$$z_1 = \frac{1}{2} (x_0 - x_1) = \frac{1}{2} (x_0, x_1) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (x_0, x_1) u_1,$$

the relations

$$x_0 = z_0 + z_1 = (z_0, z_1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \sqrt{2}\, (z_0, z_1) u_0$$

$$x_1 = z_0 - z_1 = (z_0, z_1) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \sqrt{2}\, (z_0, z_1) u_1$$

can be obtained. Therefore, the theorem holds for n = 1.

Now suppose that the theorem holds for n, then it may be proved by mathematical induction that the theorem also holds for (n + 1).

It is possible to let

$$Z_{n+1} = \begin{pmatrix} X_0, & X_1 \\ X_1, & X_0 \end{pmatrix}$$

where

$$X_0 = Z_n$$

and

$$X_1 = \begin{pmatrix} z_N, & z_{N+1}, & \ldots, & z_{2N-1} \\ z_{N+1}, & z_N, & \ldots, & z_{1\oplus(2N-1)} \\ z_{N+2}, & \cdots & & \\ \vdots & & & \\ z_{2N-1}, & z_{2N-2}, & \ldots, & z_N \end{pmatrix} \tag{2.1}$$

The relation

$$U_{n+1} = \frac{1}{\sqrt{2^{(n+1)}}} \underbrace{\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \ldots \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}}_{(n+1)}$$

$$= \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2^n}} \underbrace{\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \ldots \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \right] \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}}_{n}$$

$$= \frac{1}{\sqrt{2}} U_n \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} U_n, & U_n \\ U_n, & -U_n \end{pmatrix} \tag{2.2}$$

holds clearly.

As the theorem holds for n from the assumption,

$$\left.\begin{aligned} X_0 &= U_n \begin{pmatrix} y_0 & & & 0 \\ & y_1 & & \\ & & \ddots & \\ 0 & & & y_{N-1} \end{pmatrix} \\ y_i &= \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1}) u_i \\ z_i &= \frac{1}{\sqrt{N}}\,(y_0, y_1, \ldots, y_{N-1}) u_i \end{aligned}\right\} \qquad (2.3)$$

hold, where $0 \leq i \leq (N - 1)$.

In Eq. (2.1), letting

$$z_{i \oplus N} = z'_i$$

for $0 \leq i \leq (N - 1)$,

$$X_1 = \begin{pmatrix} z'_0, & z'_1, & \ldots, & z'_{N-1} \\ z'_1, & z'_0, & \ldots, & z'_{1\oplus(N-1)} \\ \vdots & & & \\ z'_{N-1}, & z'_{N-2}, & \ldots, & Z'_0 \end{pmatrix}$$

holds. Therefore applying the theorem to X_1,

$$\left.\begin{aligned} X_1 &= U_n \begin{pmatrix} y_N & & & 0 \\ & y_{N+1} & & \\ & & \ddots & \\ 0 & & & y_{2N-1} \end{pmatrix} U_n \\ y_{n\oplus i} &= \sqrt{N}\,(z'_0, z'_1, \ldots, z'_{N-1}) u_i = \sqrt{N}\,(z_N, z_{N+1}, \ldots, z_{1N-1}) u_i \\ z'_i &= z_{n\oplus i} = \frac{1}{\sqrt{N}}\,(y_N, y_{N+1}, \ldots, y_{2N-1}) u_i \end{aligned}\right\} \qquad (2.4)$$

hold.

Now, let

$$\left.\begin{aligned}
\Lambda_1 &= \begin{pmatrix} x_0 & & & \\ & x_1 & & 0 \\ & & \ddots & \\ & 0 & & x_{(N-1)} \end{pmatrix} \\
\Lambda_2 &= \begin{pmatrix} x_N & & & \\ & x_{N+1} & & 0 \\ & & \ddots & \\ & 0 & & x_{2N-1} \end{pmatrix}
\end{aligned}\right\} \qquad (2.5)$$

such that

$$\left.\begin{aligned}
\frac{1}{2}(\Lambda_1 + \Lambda_2) &= \begin{pmatrix} y_0 & & & \\ & y_1 & & 0 \\ & & \ddots & \\ & 0 & & y_{N-1} \end{pmatrix} \\
\frac{1}{2}(\Lambda_1 - \Lambda_2) &= \begin{pmatrix} y_N & & & \\ & y_{N+1} & & 0 \\ & & \ddots & \\ & 0 & & y_{2N-1} \end{pmatrix}
\end{aligned}\right\} \qquad (2.6)$$

Then from Eqs. (2.1) through (2.6), the relation

$$U_{n+1} \begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda \end{pmatrix} U_{n+1} = \frac{1}{2} \begin{pmatrix} U_n & U_n \\ U_n & -U_n \end{pmatrix} \begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda_2 \end{pmatrix} \begin{pmatrix} U_n, & U_n \\ U_n, & -U_n \end{pmatrix}$$

$$= \begin{pmatrix} U_n \dfrac{\Lambda_1 + \Lambda_2}{2} U_n, & U_n \dfrac{\Lambda_1 - \Lambda_2}{2} U_n \\ U_n \dfrac{\Lambda_1 - \Lambda_2}{2} U_n, & U_n \dfrac{\Lambda_1 + \Lambda_2}{2} U_n \end{pmatrix}$$

$$= \begin{pmatrix} X_0, & X_1 \\ X_1, & X_0 \end{pmatrix} = Z_{(n+1)}$$

holds. Therefore,

$$Z_{(n+1)} = U_{n+1} \begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda_2 \end{pmatrix} U_{n+1} = U_{n+1} \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{(2N-1)} \end{pmatrix} U_{n+1} \qquad (2.7)$$

holds.

From Eqs. (2.5) and (2.6),

$$x_i = y_i + y_{N+1}$$

$$x_{N+1} = y_i - y_{N+1}$$

hold, where $0 \leq i \leq (N - 1)$. Therefore, from Eqs. (2.3) and (2.4),

$$x_i = \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1})u_i + \sqrt{N}\,(z_N, z_{N+1}, \ldots, z_{2N-1})u_i$$

$$= \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1}, z_N, z_{N+1}, \ldots, z_{2N-1}) \begin{pmatrix} U_i \\ U_i \end{pmatrix} \qquad (2.8)$$

$$x_{N+i} = \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1})u_i - \sqrt{N}\,(z_N, z_{N+1}, \ldots, z_{2N-1})u_i$$

$$= \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1}, z_N, \ldots, z_{2N-1})\begin{pmatrix} u_i \\ -u_i \end{pmatrix} \qquad (2.9)$$

can be obtained, where $0 \leq i \leq (N - 1)$. Letting $U_{N+1} \equiv (v_0, v_1, \ldots, v_{2N-1})$,

$$\left.\begin{aligned} v_i &= \frac{1}{\sqrt{2}}\begin{pmatrix} u_i \\ u_i \end{pmatrix} \\ v_{N+1} &= \frac{1}{\sqrt{2}}\begin{pmatrix} u_i \\ -u_i \end{pmatrix} \end{aligned}\right\} \qquad (2.10)$$

holds, since

$$U_{n+1} = \frac{1}{\sqrt{2}}\begin{pmatrix} U_n, & U_n \\ U_n, & -U_n \end{pmatrix}$$

where $0 \leq i \leq (N - 1)$. Therefore, from Eqs. (2.8), (2.9), and (2.10),

$$\left.\begin{aligned} x_i &= \sqrt{2N}\,(z_0, z_1, \ldots, z_{2N-1})v_i \\ x_{N+i} &= \sqrt{2N}\,(z_0, z_1, \ldots, z_{2N-1})v_{N+i} \end{aligned}\right\} \qquad (2.11)$$

can be obtained where $0 \leq i \leq (N - 1)$.

From Eq. (2.11), the relation

$$(x_0, x_1, \ldots, x_{2N-1}) = \sqrt{2N}\,(z_0, z_1, \ldots, z_{2N-1})(v_0, v_1, \ldots, v_{2N-1})$$

$$= \sqrt{2N}\,(z_0, z_1, \ldots, z_{2N-1})U_{n+1}$$

holds. Therefore the relation

$$(z_0,z_1,\ldots,z_{2N-1}) = \frac{1}{\sqrt{2N}}(x_0,x_1,\ldots,x_{2N-1})U_{n+1} \qquad (2.12)$$

holds since $U_{n+1}U_{n+1} = E_{n+1}$, where E_{n+1} is the unit matrix of order n+1.

From Eq. (2.12),

$$z_i = \frac{1}{\sqrt{2N}}(x_0,x_1,\ldots,x_{2N-1})v_i$$

can be obtained, where $0 \leq i \leq (2N - 1)$.

The above description has made it clear that the theorem holds for (n + 1).

<u>Theorem 2.2</u>. In Theorem 2.1,

$$u_i^T Z_n = x_i u_i^T$$

holds, where $0 \leq i \leq (2^n - 1)$, and u_i^T means the transposed matrix of u_i.

<u>Proof</u>. From Theorem 2.1,

$$u_i^T Z = u_i^T U_n \begin{pmatrix} x_0 & & & \\ & x_1 & & 0 \\ & & \ddots & \\ & 0 & & x_{N-1} \end{pmatrix} U_n = (0,\ldots,0,1,0,\ldots,0) \begin{pmatrix} x_0 & & & \\ & x_1 & & 0 \\ & & \ddots & \\ & 0 & & x_{N-1} \end{pmatrix} U_n$$

$$= (0,\ldots,0,x_i,0,\ldots,0)U_n = (x_i u_{i0}, x_i u_{i1},\ldots,x_i u_{i(N-1)})$$

$$= x_i(u_{i0},u_{i1},\ldots,u_{i(N-1)}) = x_i u_i^T$$

can be obtained, since

$$U_n = (u_0, u_1, \ldots, u_{N-1}) = \begin{pmatrix} u_0^T \\ u_1^T \\ \vdots \\ u_{N-1}^T \end{pmatrix}$$

3. GENERAL THEORY OF MOST EFFICIENT CODES

Definition 3.1. i code

Let i be a positive integer, $0 \leq i \leq (2^n - 1)$, and let the binary expression of i be as follows:

$$i = x_{i(n-1)}2^{n-1} + \ldots + x_{i1}2 + x_{i0}.$$

Then, let the binary code $(x_{i(n-1)},\ldots,x_{i1},x_{i0})$ be called "i" code.

Notation 3.1. dist(i,j)

Let the Hamming distance between i code and j code be expressed by dist(i,j).

From Definition 2.1, Definition 3.1 and Notation 3.1,

$$\mathrm{dist}(i,j) = i \oplus j \qquad (3.1)$$

clearly holds.

Definition 3.2. Matrix H(n,p)

The matrix H(n,p) is a square matrix of order 2^n and is defined as follows:

$$H(n,p) = \begin{pmatrix} h_{00}, & h_{01}, & h_{02}, & \ldots, & h_{0(N-1)} \\ h_{10}, & h_{11}, & h_{12}, & \ldots, & h_{1(N-1)} \\ h_{20}, & h_{21}, & h_{22}, & \ldots, & h_{2(N-1)} \\ \vdots & & & & \\ h_{(N-1)0}, & h_{(N-1)1}, & h_{(N-1)2}, & \ldots, & h_{(N-1)(N-1)} \end{pmatrix} \qquad (3.2)$$

where $N = 2^n$, $n \geq p \geq 1$. Here,

$$\left.\begin{array}{l} h_{ij} = 1 \text{ when } \mathrm{dist}(i,j) < p \\ \\ h_{ij} = 0 \text{ when } \mathrm{dist}(i,j) \geq p \end{array}\right\} \qquad (3.3)$$

From Notation 3.1,

$$\mathrm{dist}(i,j) = i \oplus j = 0 \oplus (i \oplus j) = \mathrm{dist}(0, i \oplus j)$$

holds. Therefore,

$$h_{ij} = h_{0(i \oplus j)} \qquad (3.4)$$

can be obtained.

Now, define h_i as follows:

$$h_i = h_{0i} \qquad (3.5)$$

Then,

$$\begin{array}{lll} h_0 & = h_{ii} & \\ h_1 & = h_{i,i\oplus 1} & = h_{i\oplus 1,i} \\ h_2 & = h_{i,i\oplus 2} & = h_{i\oplus 2,i} \\ \vdots & & \\ h_{N-1} & = h_{i,i\oplus(N-1)} & = h_{i\oplus(N-1),i} \end{array} \qquad (3.6)$$

can be obtained for any i ($0 \leq i \leq N - 1$). Therefore, the matrix $H(n,p)$ defined by Definition 3.2 can be expressed by

$$H(N,p) = \begin{pmatrix} h_0, & h_1, & h_2, & \ldots, & h_{N-1} \\ h_1, & h_0, & h_3, & \ldots, & h_{1\oplus(N-1)} \\ \vdots & & & & \\ h_i, & h_{i\oplus 1}, & h_{i\oplus 2}, & \ldots, & h_{i\oplus(N-1)} \\ \vdots & & & & \\ h_{N-1}, & h_{N-2}, & h_{N-3}, & \ldots, & h_0 \end{pmatrix} \qquad (3.7)$$

where

$$h_0 = h_{ii} = 1 \qquad (3.8)$$

From Definition 3.2 and Eq. (3.6),

$$h_0 + h_1 + \ldots + h_{N-1} = h_{i0} + h_{i1} + \ldots + h_{i(N-1)} \equiv K(n,p) \qquad (3.9)$$

can be obtained, where

$$K(n,p) = {}_nC_0 + {}_nC_1 + \ldots + {}_nC_{p-1} \qquad (3.10)$$

<u>Example 3.1</u>

$$H(n,1) = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = E_N$$

$$K(n,1) = {}_nC_0 = 1$$

Clearly, H(n,1) is a unit matrix of order N.

Example 3.2

$$H(n,n) = \begin{pmatrix} & & & & 0 \\ & & & 0 & \\ & 1 & & & \\ & & \iddots & & \\ & 0 & & & \\ & & & 1 & \\ 0 & & & & \end{pmatrix}$$

$$K(n,n) = {}_nC_0 + {}_nC_1 + {}_nC_2 + \dots + {}_nC_{n-1} = 2^n - 1$$

Example 3.3

$$H(3,2) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$K(3,2) = {}_3C_0 + {}_3C_1 = 1 + 3 = 4$$

Theorem 3.1. The matrix $H(n,p)$ can be transformed to a diagonal matrix by the orthogonal matrix U_n, that is,

$$H(n,p) = U_n \Lambda U_n$$

and

$$\lambda_i = \sqrt{N}\ (h_0, h_1, \dots, h_{N-1}) u_i$$

$$h_i = \frac{1}{\sqrt{N}} (\lambda_0, \lambda_1, \ldots, \lambda_{N-1}) u_i$$

hold, where

$$\Lambda \equiv \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & 0 \\ & & \ddots & \\ & 0 & & \lambda_{N-1} \end{pmatrix}$$

Proof. Applying Theorem 2.1 to H(n,p), the theorem clearly holds.

Now, the most efficient coding condition is equivalent to the following condition: that is, to find a maximum m such that

$$H_0 = E_m \tag{3.11}$$

where

$$H_0 = \begin{pmatrix} h_0, & h_{i_1 \oplus i_2}, & h_{i_1 \oplus i_3}, & \ldots, & h_{i_1 \oplus i_m} \\ h_{i_2 \oplus i_1}, & h_0, & h_{i_2 \oplus i_3}, & \ldots, & h_{i_2 \oplus i_m} \\ h_{i_3 \oplus i_1}, & h_{i_3 \oplus i_2}, & h_0, & \ldots, & h_{i_3 \oplus i_m} \\ \vdots & & & & \\ h_{i_m \oplus i_1}, & h_{i_m \oplus i_2}, & h_{i_m \oplus i_3}, & \ldots, & h_0 \end{pmatrix} \tag{3.12}$$

and E_m is the unit matrix of order m.

Therefore, from Theorem 3.1, the most efficient coding condition is also equivalent to the following condition: that is, there exist u_{i_1}, u_{i_2}, ..., u_{i_m} for maximum m such that

$$H_0 = \begin{pmatrix} u_{i_1}^T \\ u_{i_2}^T \\ \vdots \\ u_{i_m}^T \end{pmatrix} \Lambda(u_{i_1}, u_{i_2}, \ldots, u_{i_m}) = E_m \tag{3.13}$$

where

$$U_n \equiv (u_0, u_1, \ldots, u_{N-1}) \equiv \begin{pmatrix} u_0^T \\ u_1^T \\ \vdots \\ u_{N-1}^T \end{pmatrix}$$

that is, u_i^T, etc., means the transposed matrix of u_i, etc.

Now, let

$$V \equiv \begin{pmatrix} u_{i_1}^T \\ u_{i_2}^T \\ \vdots \\ u_{i_m}^T \end{pmatrix} \tag{3.14}$$

Then, Eq. (3.13) leads to

$$V\Lambda V^T = E_m \qquad \text{for maximum m.} \tag{3.15}$$

As u_{i_1}, u_{i_2}, ..., u_{i_m} are column vectors belonging to the orthogonal matrix U_n,

$$VV^T = E_m \tag{3.16}$$

can be obtained. Therefore, from Eqs. (3.15) and (3.16),

$$V\Lambda V^T = VV^T = E_m$$

$$\therefore \quad V(\Lambda - E_N)V^T = 0 \qquad (3.17)$$

can be obtained, where E_N is a unit matrix of order N and the right-hand side "0" of (3.17) means the zero matrix of order m (where every element is zero).

Definition 3.3. Define the vectors $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ as follows:

$$V \equiv \begin{pmatrix} u_{i_1}^T \\ u_{i_2}^T \\ \vdots \\ u_{i_m}^T \end{pmatrix} \equiv \frac{1}{\sqrt{N}} (\zeta_0, \zeta_1, \ldots, \zeta_{N-1})$$

There exist m independent vectors among $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ since V consists of m row vectors belonging to the orthogonal matrix U_n.

Therefore, as understood clearly from Eq. (3.17) and Definition 3.3, the most efficient coding condition may be found by finding the solution of the following equation:

$$(\zeta_0, \zeta_1, \ldots, \zeta_{N-1})(\Lambda - E_N)(\zeta_0, \zeta_1, \ldots, \zeta_{N-1})^T = 0 \qquad (3.18)$$

such that the number of the independent vectors among $(\zeta_0, \zeta_1, \ldots, \zeta_{N-1})$ becomes as large as possible.

Now, some relations which hold among ζ_0, ζ_1, ..., ζ_{N-1} are described below.

Definition 3.4. Operation $\boxtimes$

Given two matrices A and B whose number of rows and columns are n and m respectively, i.e.

$$A \equiv \begin{pmatrix} a_{11}, & a_{12}, & \ldots, & a_{1m} \\ a_{21}, & a_{22}, & \ldots, & a_{2m} \\ \vdots & & & \\ a_{n1}, & a_{n2}, & \ldots, & a_{nm} \end{pmatrix} \quad \text{and} \quad B \equiv \begin{pmatrix} b_{11}, & b_{12}, & \ldots, & b_{1m} \\ b_{21}, & b_{22}, & \ldots, & b_{2m} \\ \vdots & & & \\ b_{n1}, & b_{n2}, & \ldots, & b_{nm} \end{pmatrix}$$

Define $A \boxtimes B$ as follows:

$$A \boxtimes B \equiv \begin{pmatrix} a_{11}b_{11}, & a_{12}b_{12}, & \ldots, & a_{1m}b_{1m} \\ a_{21}b_{21}, & a_{22}b_{22}, & \ldots, & a_{2m}b_{2m} \\ \vdots & & & \\ a_{n1}b_{n1}, & a_{n2}b_{n2}, & \ldots, & a_{nm}b_{nm} \end{pmatrix}$$

Definition 3.5. ξ_i

Define ξ_i as follows:

$$\sqrt{N}\, U_n \equiv (\xi_0, \xi_1, \ldots, \xi_{N-1})$$

that is, ξ_0, ξ_1, ..., ξ_{N-1} are the column vectors of $\sqrt{N}\, U_n$. Accordingly,

$$\xi_i = \sqrt{N}\, u_i \tag{3.19}$$

holds.

Theorem 3.2

$$\xi_{t \oplus \ell} = \xi_t \boxtimes \xi_\ell$$

holds, for any t, ℓ ($0 \leq t, \ell \leq N - 1$).

Proof. When n = 2,

$$\sqrt{2^2}\, U_n = \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} = \begin{pmatrix} 1, & 1, & 1, & 1 \\ 1, & -1, & 1, & -1 \\ 1, & 1, & -1, & -1 \\ 1, & -1, & -1, & 1 \end{pmatrix} = (\xi_0, \xi_1, \xi_2, \xi_3)$$

holds. Therefore

$$\xi_3 = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \boxtimes \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} = \xi_1 \boxtimes \xi_2$$

can be obtained. Therefore, the theorem holds for n = 2.

Assume that the theorem holds for n. Then, by mathematical induction, the theorem also holds in the case (n + 1).

$$\sqrt{2^{(n+1)}}\, U_{n+1} = \sqrt{2^n} \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} U_n = \begin{pmatrix} \sqrt{2^n}\, U_n, & \sqrt{2^n}\, U_n \\ \sqrt{2^n}\, U_n, & -\sqrt{2^n}\, U_n \end{pmatrix} \qquad (3.20)$$

holds, clearly.

Since the theorem holds for $\sqrt{2^n}\, U_n$ by the assumption, the theorem clearly holds for

$$\begin{pmatrix} \sqrt{2^n}\, U_n \\ \sqrt{2^n}\, U_n \end{pmatrix}$$

Therefore, letting $\sqrt{2^{(n+1)}}\ U_{n+1}$ be expressed by

$$\sqrt{2^{(n+1)}}\ U_{n+1} = (\eta_0, \eta_1, \ldots, \eta_{N-1}, \eta_N, \ldots, \eta_{2N-1}), \tag{3.21}$$

the theorem holds for

$$\begin{pmatrix} \sqrt{2^n}\ U_n \\ \sqrt{2^n}\ U_n \end{pmatrix} = (\eta_0, \eta_1, \ldots, \eta_{N-1}) \tag{3.22}$$

Since

$$\sqrt{2^n}\ U_n = (\xi_0, \xi_1, \ldots, \xi_{N-1})$$

and

$$\sqrt{2^{n+1}}\ U_{n+1} = \begin{pmatrix} \sqrt{2^n}\ U_n, & \sqrt{2^n}\ U_n \\ \sqrt{2^n}\ U_n, & -\sqrt{2^n}\ U_n \end{pmatrix},$$

$$\eta_N = \begin{pmatrix} \xi_0 \\ -\xi_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix} \tag{3.23}$$

holds. Therefore,

$$\eta_{N\oplus\ell} = \begin{pmatrix} \xi_\ell \\ -\xi_\ell \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix} \boxtimes \begin{pmatrix} \xi_\ell \\ \xi_\ell \end{pmatrix} = \eta_N \boxtimes \begin{pmatrix} \xi_\ell \\ \xi_\ell \end{pmatrix} = \eta_N \boxtimes \eta_\ell$$

holds where $0 \leq \ell \leq N - 1$.

The above discussion has shown that the theorem holds for $(n + 1)$.

<u>Theorem 3.3</u>

$$\zeta_{t\oplus\ell} = \zeta_t \boxtimes \zeta_\ell$$

holds, for any t, ℓ $(0 \leq t, \ell \leq N - 1)$.

<u>Proof</u>. The result is clear from Theorem 3.2 and Definition 3.3.

<u>Definition 3.6</u>. z_i

Define $z_0, z_1, z_2, \ldots, z_{N-1}$ as follows:

$$\sqrt{N}\, z_i = (1,1,\ldots,1)\zeta_i,$$

that is, z_i is $\frac{1}{\sqrt{N}}$ multiplied by the sum of all elements of the vectors ζ_i.

<u>Theorem 3.4</u>

$$\zeta_t^T \cdot \zeta_\ell = \sqrt{N}\, z_{t\oplus\ell}$$

for any t, ℓ $(0 \leq t, \ell \leq N - 1)$.

Proof.

$$\zeta_t^T\zeta_\ell = (1,1,\ldots,1)(\zeta_t \boxtimes \zeta_\ell) = (1,1,\ldots,1)\zeta_{t\oplus\ell} \qquad \text{(from Theorem 3.1)}$$

$$= z_{t\oplus\ell} \qquad \text{(from Definition 3.5)}$$

From Definition 3.3 and Theorem 3.4,

$$V^TV = \frac{1}{N}\begin{pmatrix} \zeta_0^T \\ \zeta_1^T \\ \vdots \\ \zeta_{N-1}^T \end{pmatrix}(\zeta_0,\zeta_1,\ldots,\zeta_{N-1}) = \frac{1}{N}\begin{pmatrix} \zeta_0^T\zeta_0, & \zeta_0^T\zeta_1, & \zeta_0^T\zeta_2, & \ldots, & \zeta_0^T\zeta_{N-1} \\ \zeta_1^T\zeta_0, & \zeta_1^T\zeta_1, & \zeta_1^T\zeta_2, & \ldots, & \zeta_1^T\zeta_{N-1} \\ \vdots & & & & \\ \zeta_{N-1}^T\zeta_0, & \zeta_{N-1}^T\zeta_1, & \zeta_{N-1,}^T\zeta_2, & \ldots, & \zeta_{N-1}^T\zeta_{N-1} \end{pmatrix}$$

$$= \frac{1}{\sqrt{N}}\begin{pmatrix} z_0, & z_1, & z_2, & \ldots, & z_{N-1} \\ z_1, & z_0, & z_3, & \ldots, & z_{1\oplus(N-1)} \\ \vdots & & & & \\ z_i, & z_{i\oplus1}, & z_{i\oplus2}, & \ldots, & z_{i\oplus(N-1)} \\ \vdots & & & & \\ z_{N-1}, & z_{N-2}, & z_{N-3}, & \ldots, & z_0 \end{pmatrix} \qquad (3.24)$$

can be obtained.

Now, following the preliminary discussion above, the most efficient coding condition is discussed below.

Definition 3.6. Define Λ', λ_i' as follows:

$$\Lambda' = \Lambda - E_N = \begin{pmatrix} \lambda_0 - 1 & & & \\ & \lambda_1 - 1 & & 0 \\ & & \ddots & \\ & 0 & & \lambda_{(N-1)} - 1 \end{pmatrix} \equiv \begin{pmatrix} \lambda'_0 & & & \\ & \lambda'_1 & & 0 \\ & & \ddots & \\ & 0 & & \lambda'_{N-1} \end{pmatrix}$$

(cf. Theorem 3.1).

Definition 3.7. Z

Define Z as follows:

$$Z = \sqrt{N}\, V^T V = \begin{pmatrix} z_0, & z_1, & z_2, & \ldots, & z_{N-1} \\ z_1, & z_0, & z_3, & \ldots, & z_{1\oplus(N-1)} \\ z_2, & z_3, & z_0, & \ldots, & z_{2\oplus(N-1)} \\ \vdots & & & & \\ z_{N-1}, & z_{N-2}, & z_{N-3}, & \ldots, & z_0 \end{pmatrix}$$

From Eq. (3.17) and Definition 3.6,

$$V\Lambda' V^T = 0 \qquad (3.25)$$

can be obtained. Therefore

$$(V^T V)\Lambda'(V^T V) = 0 \qquad (3.26)$$

can be obtained. Conversely, from (3.26) and (3.16)

$$V(V^T V)\Lambda'(V^T V)V^T = 0$$

$$\therefore \quad V\Lambda' V^T = 0$$

can be obtained. Therefore, when $VV^T = E_m$ holds, the condition (3.25) is equivalent to the condition (3.26).

From Eq. (3.26) and Definition 3.6,

$$Z\Lambda'Z = 0 \tag{3.27}$$

can be obtained. Therefore, to find the most efficient coding condition, find the maximum m such that

$$\left.\begin{aligned} VV^T &= E_m \\ Z\Lambda'Z &= 0 \end{aligned}\right\} \tag{3.28}$$

<u>Theorem 3.5</u>. When $VV^T = E_m$ and $V^TV = Z$, the rank of Z is m and the characteristic values of Z consist of "1" (m times) and "0" (N - m times).

<u>Proof</u>. Since $VV^T = E_m$ holds,

$$\det(\lambda E_m - VV^T) = (\lambda - 1)^m$$

can clearly be obtained.

On the other hand, since

$$\det(\lambda E_N - V^TV) = \{\det(\lambda E_m - VV^T)\}\lambda^{N-m}$$

holds generally,

$$\det(\lambda E_N - V^TV) = (\lambda - 1)^m\lambda^{(N-m)} \tag{3.29}$$

can be obtained.

Applying Theorem 2.1 to V^TV,

$$Z = \sqrt{N}\, V^T V = \begin{pmatrix} z_0, & z_1, & \ldots, & z_{N-1} \\ \vdots & & & \\ z_i, & z_{i\oplus 1}, & \ldots, & z_{i\oplus(N-1)} \\ \vdots & & & \\ z_{N-1}, & z_{N-2}, & \ldots, & z_0 \end{pmatrix} = U_n \begin{pmatrix} x_0 & & & \\ & x_1 & & 0 \\ & & \ddots & \\ & 0 & & x_{(N-1)} \end{pmatrix} U_n \tag{3.30}$$

can be obtained.

From Eqs. (3.29) and (3.30), the rank of Z is m and the characteristic values of Z, i.e., x_0, x_1, ..., x_{N-1} consist of "1" (m times) and "0" (N - m times).

From Theorem 3.5, finding the condition for the most efficient codes can also be reduced to finding the solution of equations

$$\left.\begin{aligned} VV^T &= E_m \\ Z\Lambda'Z &= 0 \end{aligned}\right\} \tag{3.31}$$

with the maximum rank of Z.

Remark 3.1. From (3.30),

$$x_i = \sqrt{N}\,(z_0, z_1, \ldots, z_{N-1}) u_i$$

can be obtained. If $x_{i_1} = x_{i_2} = \ldots = x_{i_m} = 1$ and the other $x_i = 0$, i_1 code, i_2 code, ..., i_m code are all of the most efficient codes.

4. CALCULATION AND SOME PROPERTIES OF EACH λ_i

The value of each λ_i is given by the formula of Theorem 3.1, i.e.,

$$\lambda_i = \sqrt{N}\ (h_0, h_1, \ldots, h_{N-1})u_i$$

where each h_i is decided uniquely by the value of n and p.

Another method of calculating each λ_i and some properties of λ_i are discussed below.

Theorem 4.1. $p = 1$ if and only if $\lambda_0 = \lambda_1 = \ldots = \lambda_{N-1} = 1$.

Proof. If $\lambda_0 = \lambda_1 = \ldots = \lambda_{N-1} = 1$, from Theorem 3.1,

$$h_i = \frac{1}{\sqrt{N}} (\lambda_0, \lambda_1, \ldots, \lambda_{N-1})u_i = \frac{1}{\sqrt{N}} (1, 1, \ldots, 1)u_i = \begin{cases} 1 \text{ when } i = 0 \\ 0 \text{ when } i \neq 0 \end{cases}$$

can be obtained. Therefore,

$$H(n,p) = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

can be obtained. Therefore, $p = 1$.

Conversely, if $p = 1$,

$$h_0 = 1, \quad h_i = 0 \quad \text{for } i \neq 0$$

can be obtained. Therefore,

$$\lambda_i = \sqrt{N}\ (1, 0, 0, \ldots, 0)u_i = 1 \text{ for any } i \qquad (0 \leq i \leq N - 1)$$

Therefore, the theorem holds.

Theorem 4.2

$$\lambda_0 + \lambda_1 + \ldots + \lambda_{N-1} = N$$

$$\lambda_0^2 + \lambda_1^2 + \ldots + \lambda_{N-1}^2 = NK(n,p)$$

Proof. From Theorem 3.1,

$$\lambda_i = \sqrt{N}\,(h_0,h_1,\ldots,h_{N-1})u_i$$

$$\therefore \quad \lambda_0 + \lambda_1 + \ldots + \lambda_{N-1} = \sqrt{N}\,(h_0,h_1,\ldots,h_{N-1})(u_0 + u_1 + \ldots + u_{N-1})$$

$$= \sqrt{N}\,(h_0,h_1,\ldots,h_{N-1}) \begin{pmatrix} \sqrt{N} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = Nh_0 = N$$

can be obtained. From Theorem 3.1,

$$H(n,p) = U_n \Lambda U_n$$

$$\therefore \quad H^2 = U_n \Lambda^2 U_n$$

$$\therefore \quad \lambda_i^2 = \sqrt{N}\,(\mathcal{L}_0^T\mathcal{L}_0, \mathcal{L}_0^T\mathcal{L}_1, \ldots, \mathcal{L}_0^T\mathcal{L}_{N-1})u_i$$

can be obtained, where

$$H(n,p) \equiv (\mathcal{L}_0,\mathcal{L}_1,\ldots,\mathcal{L}_{N-1}) = \begin{pmatrix} \mathcal{L}_0^T \\ \mathcal{L}_1^T \\ \vdots \\ \mathcal{L}_{N-1}^T \end{pmatrix}$$

Therefore,

$$\lambda_0^2 + \lambda_1^2 + \ldots + \lambda_{N-1}^2 = \sqrt{N}\,(\mathcal{L}_0^T\mathcal{L}_0, \mathcal{L}_0^T\mathcal{L}_1, \ldots, \mathcal{L}_0^T\mathcal{L}_{N-1})(u_0 + u_1 + \ldots + u_{N-1})$$

$$= \sqrt{N}\,(\mathcal{L}_0^T\mathcal{L}_0, \mathcal{L}_0^T\mathcal{L}_1, \ldots, \mathcal{L}_0^T\mathcal{L}_{N-1})\begin{pmatrix} \sqrt{N} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$= N\mathcal{L}_0^T\mathcal{L}_0 = N(h_0 + h_1 + \ldots + h_{N-1}) = NK(n,p)$$

Theorem 4.3. The following relations hold:

(1) $\lambda_0 = K(n,p)$

(2) Any λ_i for $1 \leq i \leq N - 1$ are

$$\lambda_0 = K(n,p) \geq \lambda_i = \text{integer}$$

where the equality holds if and only if $p = 1$.

Proof. From Theorem 3.1,

$$\lambda_i = \sqrt{N}\,(h_0, h_1, \ldots, h_{N-1})u_i = (h_0, h_1, \ldots, h_{N-1})\xi_i = \text{integer}$$

can be obtained.

Since each h_i is equal to 1 or 0,

$$(h_0, h_1, \ldots, h_{N-1})u_0 \geq (h_0, h_1, \ldots, h_{N-1})u_i$$

and

$$\lambda_0 = \sqrt{N}\,(h_0, h_1, \ldots, h_{N-1})u_0 = h_0 + h_1 + \ldots + h_{N-1} = K(n,p)$$

$$\therefore \quad \lambda_0 = K(n,p) \geq \lambda_i$$

can be obtained.

Suppose that there exists i, $1 \leq i \leq (N - 1)$, such that

$$\lambda_0 = \lambda_i .$$

Then,

$$(h_0, h_1, \ldots, h_{N-1})u_0 = (h_0, h_1, \ldots, h_{N-1})u_i$$

$$\therefore \quad (h_0, h_1, \ldots, h_{N-1})(\xi_0 - \xi_i) = 0$$

can be obtained.

Since

$$(\xi_0 - \xi_i) = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ \pm 1 \\ \pm 1 \\ \vdots \\ \pm 1 \end{pmatrix}$$

each element of $(\xi_0 - \xi_i)$ is equal to 2 or 0, i.e., non-negative, and there exist elements except the first row element such that the value is equal to 2. (Clearly, there is no case except $p = 1$ for $n = 1$.) Therefore,

$$(h_0, h_1, \ldots, h_{N-1})(\xi_0 - \xi_i) = 0$$

holds if and only if $h_0 = 1$, $h_1 = h_2 = \ldots = h_{N-1} = 0$. This is the case where $p = 1$.

Theorem 4.4

$$\begin{array}{llll}
\lambda_{r_1} & = \lambda_{r_2} & = \ldots = \lambda_{r_n} \\
\lambda_{r_1+r_2} & = \lambda_{r_1+r_3} & = \ldots = \lambda_{r_{n-1}+r_n} \\
\lambda_{r_1+r_2+r_3} & = \lambda_{r_1+r_2+r_4} & = \ldots = \lambda_{r_{n-2}+r_{n-1}+r_n} \\
\vdots & & \\
\lambda_{r_1+r_2+\ldots+r_{n-1}} & = \lambda_{r_1+r_2+\ldots+r_{n-2}+r_n} & = \ldots = \lambda_{r_2+r_3+\ldots+r_n}
\end{array}$$

where

$$r_1 = 2^{n-1},\ r_2 = 2^{n-2},\ \ldots,\ r_n = 2^0 = 1.$$

Proof. Consider any permutation of the correspondence

$$\begin{pmatrix} x_{i(n-1)}, & x_{i(n-2)}, & \ldots, & x_{i1}, & x_{i0} \\ x_{is_{(n-1)}}, & x_{is_{(n-2)}}, & \ldots, & x_{is_1}, & x_{is_0} \end{pmatrix}$$

where

$$i = x_{i(n-1)}2^{n-1} + x_{i(n-2)}2^{n-2} + \ldots + x_{i1}2 + x_{i0}$$

that is, any change of the column position of codes.

From the definition of H(n,p), i.e., Definition 3.2, H(n,p) is invariant under this change.

In $H(n,p) = U_n \Lambda U_n$, U_n is also invariant under this change.

Suppose that Λ becomes Ψ under this change. Then,

$$H(n,p) = U_n \Lambda U_n = U_n \Psi U_n$$

holds. Therefore,

$$\Lambda = \Psi$$

can be obtained. Therefore, Λ has to be also invariant under this change.

As mentioned above,

$$\begin{array}{lll}
\lambda_{r_1} & = \lambda_{r_2} & = \ldots = \lambda_{r_n} \\
\lambda_{r_1+r_2} & = \lambda_{r_1+r_3} & = \ldots = \lambda_{r_{n-1}+r_n} \\
\vdots & & \\
\lambda_{r_1+r_2+\ldots+r_{n-1}} & = \lambda_{r_1+\ldots+r_{n-2}+r_n} & = \ldots = \lambda_{r_2+r_3+\ldots+r_n}
\end{array}$$

must hold.

<u>Definition 4.1</u>. Extension of the definition of $H(n,p)$ (cf., Definition 3.2).

Define $H(n,p)$ of the matrix of order 2^n where $n < p$ and $p = 0$ as follows:

$$H(n,p) = \begin{pmatrix} 1, & 1, & \ldots, & 1 \\ 1, & 1, & \ldots, & 1 \\ \vdots & & & \\ 1, & 1, & \ldots, & 1 \end{pmatrix} \qquad \text{when } n < p,$$

$$H(n,0) = \begin{pmatrix} 0, & 0, & \ldots, & 0 \\ 0, & 0, & \ldots, & 0 \\ \vdots & & & \\ 0, & 0, & \ldots, & 0 \end{pmatrix} \qquad \text{when } p = 0.$$

Theorem 4.5

$$H(n,p) = \begin{pmatrix} H(n-1,p), & H(n-1,p-1) \\ H(n-1,p-1), & H(n-1,p) \end{pmatrix}$$

holds where $n \geq 0$, $p \geq 0$.

Proof. It is clear from Definition 3.2 and Definition 4.1.

Definition 4.2. Extension of the definition K(n,p) (cf., (3.9))

In general, define K(n,p) as follows:

$$K(n,p) = {}_nC_0 + {}_nC_1 + \dots + {}_nC_{p-1} \qquad \text{when } n \geq p \geq 1,$$

$$K(n,p) = 2^n \qquad \text{when } 0 \leq n < p,$$

$$K(n,o) = 0 \qquad \text{when } n \geq o,\ p = o.$$

From Definition 4.2,

$$\left.\begin{aligned} K(n,n) &= 2^n - 1 \\ K(o,p) &= 2^o = 1 \qquad \text{for } p > o \end{aligned}\right\} \tag{4.1}$$

can be obtained.

Remark 4.1. It is clear that the theorems, etc., presented until now also hold if the definitions of H(n,p) and K(n,p) are extended like Definitions 4.1 and 4.2.

Theorem 4.6

$$\lambda_0 = K(n,p)$$

$$\lambda_0 + \lambda_{r_1} = 2K(n-1,p)$$

$$\lambda_0 + {}_2C_1\lambda_{r_1} + \lambda_{r_1+r_2} = 2^2K(n-2,p)$$

$$\lambda_0 + {}_3C_1\lambda_{r_1} + {}_3C_2\lambda_{r_1+r_2} + \lambda_{r_1+r_2+r_3} = 2^3K(n-3,p)$$

$$\vdots$$

$$\lambda_0 + {}_sC_1\lambda_{r_1} + {}_sC_2\lambda_{r_1+r_2} +\dots+ {}_sC_{s-1}\lambda_{r_1+r_2+\dots+r_{s-1}} + \lambda_{r_1+r_2+\dots+r_s} = 2^sK(n-s,p)$$

$$\vdots$$

$$\lambda_0 + {}_nC_1\lambda_{r_1} + {}_nC_2\lambda_{r_1+r_2} +\dots+ {}_nC_{n-1}\lambda_{r_1+r_2+\dots+r_{n-1}} + \lambda_{r_1+r_2+\dots+r_n} = 2^nK(o,p) = 2^n$$

holds.

Proof.

$$H(n,p) = U_n\Lambda U_n = \frac{1}{2}\begin{pmatrix} U_{n-1}, & U_{n-1} \\ U_{n-1}, & -U_{n-1} \end{pmatrix}\begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda_2 \end{pmatrix}\begin{pmatrix} U_{n-1}, & U_{n-1} \\ U_{n-1}, & -U_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} U_{n-1}\dfrac{\Lambda_1 + \Lambda_2}{2}U_{n-1}, & U_{n-1}\dfrac{\Lambda_1 - \Lambda_2}{2}U_{n-1} \\ U_{n-1}\dfrac{\Lambda_1 - \Lambda_2}{2}U_{n-1}, & U_{n-1}\dfrac{\Lambda_1 + \Lambda_2}{2}U_{n-1} \end{pmatrix}$$

holds, where

$$\Lambda = \begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda_2 \end{pmatrix}$$

On the other hand, since

$$H(n,p) = \begin{pmatrix} H(n-1,p), & H(n-1,p-1) \\ H(n-1,p-1), & H(n-1,p) \end{pmatrix}$$

holds from Theorem 4.5,

$$H(n-1,p) = U_{n-1} \frac{\Lambda_1 + \Lambda_2}{2} U_{n-1} \tag{4.2}$$

can be obtained. Therefore, from Theorem 4.3 and Eq. (4.2),

$$\frac{\lambda_0 + K_{r_1}}{2} = K(n-1,p)$$

$$\lambda_0 + \lambda_{r_1} = 2K(n-1,p)$$

must hold, where $r_1 = 2^{n-1}$.

Similarly, since

$$H(n-1,p) = \begin{pmatrix} H(n-2,p) & H(n-2,p-1) \\ H(n-2,p-1), & H(n-2,p) \end{pmatrix}$$

holds from Theorem 4.5,

$$\lambda_0 + \lambda_{r_1} + \lambda_{r_2} + \lambda_{r_1+r_2} = 2^2K(n-2,p)$$

$$\therefore \quad \lambda_0 + {}_2C_1\lambda_{r_1} + \lambda_{r_1+r_2} = 2^2K(n-2,p) \tag{4.4}$$

must hold since

$$\lambda_{r_1} = \lambda_{r_2}$$

holds from Theorem 4.4, where $r_2 = 2^{n-2}$.

Similarly, in general,

$$\lambda_0 + {}_sC_1\lambda_{r_1} + {}_sC_2\lambda_{r_1+r_2} + \ldots + {}_sC_{s-1}\lambda_{r_1+r_2+\ldots+r_{s-1}} + \lambda_{r_1+r_2+\ldots+r_s} = 2^sK(n-s,p)$$

can be obtained, where $r_i = 2^{n-i}$ for $1 \leq i \leq n$ and $1 \leq s \leq n$.

Accordingly, this theorem holds.

5. SOME PROPERTIES OF ζ

An independent vector in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, is not determined uniquely. Therefore, independence is defined as follows.

Definition 5.1. Independence of the vector ζ_i

Let ζ_i be called an independent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ when it satisfies the following condition: ζ_i cannot be expressed as a linear combination of $\zeta_0, \zeta_1, \ldots, \zeta_{i-1}$, i.e., there do not exist $a_0, a_1, \ldots, a_{i-1}$ such that

$$\zeta_i = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1},$$

where $a_0, a_1, \ldots, a_{i-1}$ are real numbers.

Definition 5.2. Dependence of the vector of ζ_i

Let ζ_i be called a dependent vector in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, when it satisfies the following condition: ζ_i can be expressed as a linear combination of $\zeta_0, \zeta_1, \ldots, \zeta_{i-1}$, i.e., there exist $a_0, a_1, \ldots, a_{i-1}$ such that

$$\zeta_i = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1},$$

where $a_0, a_1, \ldots, a_{i-1}$ are real numbers.

Definition 5.3. Generator of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$

Let $\zeta_0, \zeta_1, \zeta_2, \zeta_{2^2}, \ldots, \zeta_{2^{n-1}}$ be called generators of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

Theorem 5.1. When ζ_i $(0 \leq i \leq 2^s - 1)$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, each of ζ_{2^t+i} $(n - 1 \geq t > s)$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

Proof. Since ζ_i is a dependent vector, ζ_i can be expressed by

$$\zeta_i = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1}$$

where $0 \leq i \leq (2^s - 1)$.

Therefore,

$$\zeta_i \boxtimes \zeta_{2^t} = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1}) \boxtimes \zeta_{2^t}$$

$$\therefore \quad \zeta_{2^t+i} = a_0\zeta_{2^t} + a_1\zeta_{2^t+1} + \ldots + a_{i-1}\zeta_{2^t+(i-1)}$$

where $2^{n-1} \geq 2^t > 2^s$.

Therefore, from Definition 5.2, ζ_{2^t+i} is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}.

Theorem 5.2. When a generator ζ_{2^s} is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}, every ζ_{2^s+i} $(0 \leq i \leq 2^{(s+1)} - 1)$ is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}.

Proof. Since ζ_{2^s} is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}, ζ_{2^s} can be expressed by

$$\zeta_{2^s} = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{(2^s-1)}\zeta_{(2^s-1)}.$$

Therefore,

$$\zeta_{2^s} \boxtimes \zeta_i = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{(2^s-1)}\zeta_{(2^s-1)}) \boxtimes \zeta_i$$

$$\therefore \quad \zeta_{2^s \oplus i} = a_0\zeta_i + a_1\zeta_{i\oplus 1} + \ldots + a_{(2^s-1)}\zeta_{i\oplus(2^s-1)}$$

can be obtained. Since $0 \leq i \oplus j \leq (2^s - 1)$ for $0 \leq j \leq (2^s - 1)$ holds, ζ_{2^s+i} is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}.

Theorem 5.3. When ζ_{2i} is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, ζ_{2i+1} is also a dependent vector.

Proof. Since ζ_{2i} is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$,

$$\zeta_{2i} = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2i-1}\zeta_{2i-1}$$

$$\therefore \quad \zeta_{2i} \boxtimes \zeta_1 = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2i-1}\zeta_{2i-1}) \boxtimes \zeta_1$$

can be obtained. Here since

$$0 \leq j \oplus 1 \leq 2i - 1 \qquad \text{for } 0 \leq j \leq (2i - 1),$$

can be obtained. Therefore, ζ_{2i+1} is also a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

In general, the following theorem holds as an extension of Theorem 5.1 and Theorem 5.2.

Theorem 5.4. When $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}}$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}+i}$ is also a dependent vector, for any i, $0 \leq i \leq 2^{s_\ell} - 1$ and $s_0 > s_1 > s_2 > \ldots > s_\ell \geq 1$.

Proof. Since $\zeta_{2^{s_1}+2^{s_2}+2^{s_\ell}}$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$,

$$\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}} = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}$$

$$\therefore (\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}}) \boxtimes \zeta_1 = (a_0\zeta_0+a_1\zeta_1+\ldots+a_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{2_\ell}-1}) \boxtimes \zeta_i$$

can be obtained. Since

$$0 \leq j \oplus i \leq 2^{s_1} + 2^{s_2} + \ldots + 2^{s_\ell} - 1$$

holds for $0 \leq j \leq 2^{s_1} + 2^{s_2} + \ldots + 2^{s_\ell} - 1$ and for $0 \leq i \leq 2^{s_\ell} - 1$,

$$\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}+i} = a_0\zeta_i + \ldots + a_{2^{s_0}+2^{s_1}+\ldots+2^{s_\ell}-1}\zeta_{(2^{s_0}+2^{s_1}+2^{s_\ell}-1)\oplus i}$$

can be obtained, where the right-hand side is the linear combination of ζ_0, ζ_1, ..., $\zeta_{2^{s_0}+2^{s_1}+\ldots+2^{s_\ell}-1}$.

Therefore, $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}+i}$ is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1}.

Theorem 5.5. When ζ_{2^s-1} is an independent vector of ζ_0, ζ_1, ..., ζ_{N-1}, ζ_i is also an independent vector for any i, $1 \leq i \leq (2^s - 1)$.

Proof. Suppose that there exists a dependent vector ζ_i of ζ_0, ζ_1, ..., ζ_{N-1}. Then

$$\zeta_i = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1}$$

can be obtained, where $1 \leq i \leq 2^s - 1$.

Now,

$$\zeta_i \boxtimes \zeta_{(2^s-1)\oplus i} = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{i-1}\zeta_{i-1}) \boxtimes \zeta_{(2^s-1)\oplus i}$$

accordingly,

$$\zeta_{(2^s-1)} = a_0\zeta_{(2^s-1)\oplus i} + a_1\zeta_{1\oplus(2^s-1)\oplus i} + \ldots + a_{i-1}\zeta_{(i-1)\oplus(2^s-1)\oplus i} \qquad (5.1)$$

holds. Since

$$0 \leq j \oplus (2^s - 1) \oplus i < 2^s - 1$$

holds for any j $(0 \leq j < 2^s - 1)$ and for any i $(1 \leq i < 2^s - 1)$ and for $j \leq (i - 1)$, the right-hand side of Eq. (5.1) is a linear combination of some of $\zeta_0, \zeta_1, \ldots, \zeta_{(2^s-1)}$. Therefore, $\zeta_{(2^s-1)}$ becomes a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

This contradicts the assumption of the theorem. Therefore, ζ_i is also an independent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

In general, the following theorem holds as an extension of Theorem 5.5.

<u>Theorem 5.6</u>. When $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}$ is an independent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+i}$ is also an independent vector for any i, where $s_1 > s_2 > \ldots > s_\ell \geq 1$ and $1 \leq i \leq (2^{s_\ell} - 1)$.

<u>Proof</u>. Suppose that there exists the dependent vector $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+i}$ of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ where $1 \leq i < 2^{s_\ell} - 1$. Then

$$\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+i} = a_0\zeta_0 + a_1\zeta_1 + \ldots$$
$$+ a_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+i}\,\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+(i-1)}$$

accordingly,

$$(\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_{(\ell-1)}}+i}) \boxtimes \zeta_{(2^{2_\ell}-1)\oplus i} = (a_0\zeta_0 + \ldots$$
$$+ a_{2^{s_1}+\ldots+2^{s_{(\ell-1)}}+i}\,\zeta_{2^{s_1}+\ldots+2^{s_{(\ell-1)}}+(i-1)}) \boxtimes \zeta_{(2^{s_\ell}-1)\oplus i}$$

can be obtained. Therefore,

$$\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1} = a_0\zeta_{(2^{s_\ell}-1)\oplus i} + a_1\zeta_{1\oplus(2^{s_\ell}-1)\oplus i} + \ldots$$

$$+ a_{2^{s_1}+2^{s_2}+\ldots+2^{s(\ell-1)}+i}\,\zeta_{\{2^{s_1}+\ldots+2^{s(\ell-1)}+(i-1\}\oplus(2^{s_\ell}-1)\oplus i} \qquad (5.2)$$

can be obtained. Since

$$0 \leq \{2^{s_1} + 2^{s_2} + \ldots + 2^{s_{\ell-1}} + j\} \oplus (2^{s_\ell} - 1) \oplus i < (2^{s_1} + 2^{s_2} + \ldots + 2^{s_\ell} - 1)$$

holds for any $j \leq (i - 1)$, where

$$0 \leq j < 2^{s_\ell} - 1$$

and

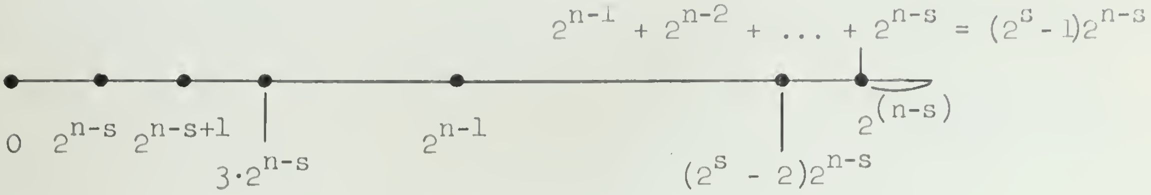
$$1 \leq i < 2^{s_\ell} - 1$$

Therefore, the right-hand side of Eq. (5.2) is a linear combination of some of $\zeta_0, \zeta_1, \ldots, \zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-2}$. Therefore, $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}$ becomes a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

This contradicts the assumption of this theorem. Therefore, $\zeta_{2^{s_1}+2^{s_2}+\ldots+2^{s_\ell}-1}$ is also an independent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

Theorem 5.7. When $\zeta_{2^{n-1}+2^{n-2}+\ldots+2^{n-s}}$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, it can be expressed as a linear combination of ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, $\zeta_{3\cdot 2^{n-s}}$, $\ldots$, $\zeta_{(2^s-2)2^{n-s}}$, that is,

$$\zeta_{2^{n-1}+2^{n-2}+\ldots+2^{n-s}} = a_0\zeta_0 + a_1\zeta_{2^{n-s}} + \ldots + a_{(2^s-2)}\zeta_{(2^s-2)2^{n-s}}$$



where $1 < s \leq n$. Accordingly

$$\zeta_{2^{n-1}+2^{n-2}+\ldots+2^{n-s}+i} = a_0\zeta_i + a_1\zeta_{2^{n-s}+i} + a_2\zeta_{2\cdot 2^{n-s}+i} + \ldots + a_{(2^s-2)}\zeta_{(2^s-2)2^{n-s}+i} \tag{5.3}$$

can be obtained for any i $(0 \leq i \leq (2^{n-s} - 1))$.

<u>Proof</u>. From Theorem 5.2, $\zeta_{2^{n-1}+2^{n-2}+\ldots+2^{n-s}+i}$ is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1} for any i $(0 \leq i \leq (2^{n-s} - 1))$. Therefore, there exist at least 2^{n-s} dependent vectors in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$.

Now the generators in ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, $\zeta_{3\cdot 2^{n-s}}$, ..., $\zeta_{(2^s-s)2^{n-s}}$, are ζ_0, $\zeta_{2^{n-1}}$, $\zeta_{2^{n-2}}$, ..., $\zeta_{2^{n-s}}$.

Since

$$(\zeta_0, \zeta_{2^{n-1}}, \ldots, \zeta_{2^{n-s}}) = \left(\begin{array}{cccc} 1 & 1 & \cdots & \left.\begin{array}{c} 1 \\ 1 \end{array}\right\} 2^{(n-s)} \\ & \vdots & & \\ \vdots & & & -1 \\ \vdots & 1 & & -1 \\ \hdashline \vdots & -1 & & \\ & \vdots & & \\ 1 & -1 & & \\ \hdashline 1 & 1 & & \\ & \vdots & & \\ \vdots & & & \\ & 1 & & \\ \hdashline \vdots & -1 & & \\ & \vdots & & \\ 1 & -1 & & \end{array}\right)$$

the vectors ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, ..., $\zeta_{(2^s-2)2^{n-s}}$ are constructed by the 2^{n-s} quantum vectors

$$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix}$$

Therefore, there exist at most $\frac{2^n}{2^{n-s}} = 2^s$ independent vectors in ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, ..., $\zeta_{(2^s-1)2^{n-s}}$. Here, if and only if the number of elements of each ζ is 2^n, the number of the independent vectors is 2^s.

From the description above, there exist at least 2^{n-s} dependent vectors. Therefore, the number of elements of each ζ is equal to or less than $2^n - 2^{(n-s)}$. Therefore, the number of independent vectors in ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, ..., $\zeta_{(2^s-1)2^s}$ is at most $\frac{2^n - 2^{n-s}}{2^{n-s}} = 2^s - 1$.

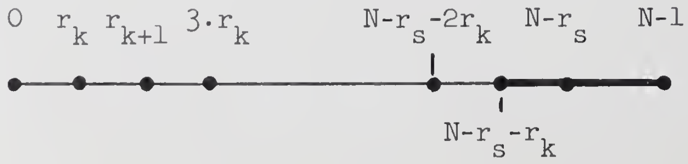
On the other hand, the number of vectors of ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, ..., $\zeta_{(2^s-1)2^{n-s}}$ is 2^s. Therefore, $\zeta_{(2^s-1)2^{n-s}} = \zeta_{2^{n-1}+2^{n-2}+\dots+2^{n-2}}$ can be expressed as a linear combination of ζ_0, $\zeta_{2^{n-s}}$, $\zeta_{2^{n-s+1}}$, ..., $\zeta_{(2^s-2)2^{n-s}}$.

Since

$$2^{n-1},\ 2^{n-2},\ \dots,\ 2^{n-s} > i$$

holds for any i $(0 \leq i \leq (2^{n-s} - 1))$, the subscript of each ζ of the right-hand side of Eq. (5.3) is between 0 and $(2^{n-2} + 2^{n-2} + \dots + 2^{n-s} - 1)$. Therefore, Eq. (5.3) holds.

Theorem 5.8



When every ζ_i for $N - r_s - r_k \leq i \leq N - 1$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, $\zeta_{N-r_s-r_k}$ can be expressed as a linear combination of ζ_0, ζ_{r_k}, $\zeta_{r_{(k+1)}}$, $\zeta_{3\cdot r_k}$, $\ldots$, $\zeta_{N-r_s-2r_k}$ where $r_1 > r_s > r_k$ and $r_1 = 2^{n-1}$, $r_2 = 2^{n-2}$, $\ldots$, $r_s = 2^{n-s}$, $\ldots$, $r_k = 2^{n-k}$, that is

$$\zeta_{N-r_s-r_k} = a_0\zeta_0 + a_1\zeta_{r_k} + a_2\zeta_{2\cdot r_k} + \ldots + a_{N-r_s-2r_k/r_k}\zeta_{N-r_s-2r_k}$$

Accordingly,

$$\zeta_{(N-r_s-r_k)+i} = a_0\zeta_i + a_1\zeta_{r_k+i} + \ldots + a_{N-r_s-2r_k/r_k}\zeta_{N-r_s-2r_k+i} \qquad (5.4)$$

can be obtained for any i $(0 \leq i \leq (r_k - 1))$.

Proof. As in the proof of Theorem 5.7, ζ_0, ζ_{r_k}, ζ_{2r_k}, $\ldots$, $\zeta_{N-r_s-2r_k}$, $\zeta_{N-r_s-r_k}$ are constructed by the quantum vectors

$$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix}$$

each with r_k elements. Therefore, the number of independent vectors in ζ_0, ζ_{r_k}, $\zeta_{2\cdot r_k}$, $\ldots$, ζ_{N-r_k} is at most $\frac{2^n}{r_k}$. Further, if and only if the number of elements of each ζ is 2^n, the number of independent vectors in ζ_0, ζ_{r_k}, $\ldots$, ζ_{N-r_k} is $\frac{2^n}{r_k}$.

From the assumption of this theorem, the number of dependent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ is at least $r_s + r_k$. Therefore, the number of elements of each ζ is not more than $N - r_s - r_k$. Therefore, the number of independent vectors in ζ_0, ζ_{r_k}, $\zeta_{2\cdot r_k}$, $\ldots$, ζ_{N-r_k} is not more than $\frac{N - r_s - r_k}{r_k} = \left(\frac{N - r_s}{r_k} - 1\right)$.

On the other hand, the number of $\zeta_0, \zeta_{r_k}, \zeta_{2r_k}, \ldots, \zeta_{N-r_s-r_k}$ is $\frac{N - r_s}{r_k}$. Therefore, $\zeta_{N-r_s-r_k}$ can be expressed as a linear combination of $\zeta_0, \zeta_{r_k}, \zeta_{2r_k}, \ldots, \zeta_{N-r_s-2r_k}$.

Since

$$r_1, r_2, \ldots, r_s, \ldots, r_k > i \geq 0$$

holds for any i $(0 \leq i \leq (r_{k-1}))$, the subscript of each ζ of the right-hand side of Eq. (5.4) is between 0 and $(n - r_s - r_k - 1)$. Therefore, Eq. (5.4) holds.

Theorem 5.9. Let $n_0, n_1, n_2, \ldots, n_{(2^{(n-k)}-1)}$ be as follows:

n_0: the number of independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{(2^k-1)}$

n_1: the number of independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in $\zeta_{2^k}, \zeta_{2^k+1}, \zeta_{2^k+2}, \ldots, \zeta_{2^{(k+1)}-1}$

n_2: the number of independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in $\zeta_{2^{(k+1)}}, \zeta_{2^{(k+1)}+1}, \zeta_{2^{(k+1)}+2}, \ldots, \zeta_{3\cdot 2^k-1}$

$n_{(2^{(n-k)}-1)}$: the number of independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in $\zeta_{N-2^k}, \zeta_{N-2^k+1}, \ldots, \zeta_{N-1}$.

Then

$$n_0 \geq n_1 \geq n_2 \geq \ldots \geq n_{(2^{(n-k)}-1)} \geq 0$$

holds, where $0 \leq k \leq n - 1$.

Proof. It is clear.

Theorem 5.10. Rearrange the generators $\zeta_0, \zeta_1, \zeta_2, \zeta_{2^2}, \ldots, \zeta_{2^{n-1}}$ of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in the order: $\zeta_0, \zeta_{2^{n-1}}, \zeta_1, \zeta_2, \ldots, \zeta_{2^{n-2}}$. Then the order of vectors after $\zeta_{2^{n-2}}$ becomes: $\ldots, \zeta_{2^{n-2}}, \zeta_{2^{n-1}+2^{n-2}}, \zeta_{2^{n-2}+1}, \zeta_{2^{n-1}+2^{n-2}+1}, \zeta_{2^{n-2}+2}, \zeta_{2^{n-1}+2^{n-2}+2}, \ldots, \zeta_{2^{n-2}-2}, \zeta_{2^n-2}, \zeta_{2^{n-1}-1}, \zeta_{2^n-1}$.

Proof. The vectors after $\zeta_{2^{n-1}}$ in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ have always the factor 2^{n-1} in their subscripts and have any combination from $2^{n-2}, 2^{n-3}, \ldots, 2, 1$ in their subscripts. Therefore, applying the substitution:

$$\begin{pmatrix} 0, & 1, & 2, & 2^2, & \ldots, & 2^{n-2}, & 2^{n-1} \\ 0, & 2^{n-1}, & 1, & 2^1, & \ldots, & 2^{n-3}, & 2^{n-2} \end{pmatrix}$$

to the generators of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, the vectors after the 2^{n-1}th have always the factor 2^{n-2} in their subscripts and have any combination from $2^{n-1}, 1, 2, 2^2, \ldots, 2^{n-3}$ in their subscripts. That is, all vectors after the $2^{(n-1)}$th from $\zeta_{2^{n-2}}$ to $\zeta_{(2^{(n-1)}-1)}$ and from $\zeta_{2^{n-1}+2^{n-2}}$ to ζ_{N-1} in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ are arranged in the new arrangement. The adjacent vectors

$$\zeta_{2^{n-1}+f(2^{n-2},2^{n-3},\ldots,2^1)}, \zeta_{2^{n-1}+f(2^{n-2},2^{n-3},\ldots,2^1)+1}$$

in $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ (where $f(2^{n-2},2^{n-3},\ldots,2^1)$ means that some combination from $2^{n-2}, 2^{n-3}, \ldots, 2^1$ is added) become respectively the adjacent vectors

$$\zeta_{2^{n-2}+f(2^{n-3},2^{n-4},\ldots,2,1)}, \zeta_{2^{n-2}+f(2^{n-3},2^{n-4},\ldots,2,1)+2^{n-1}}$$

after the substitution.

Therefore, this theorem holds.

Example 5.1

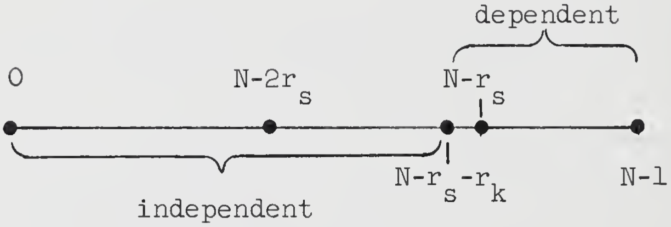
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,

is rearranged to

0, 8, 1, 9, 2, 10, 3, 11, 4, 12, 5, 13, 6, 14, 7, 15,

after the substitution.

Theorem 5.11.



When every ζ_i for $N - r_s - r_k \le i \le N - 1$ is an independent vector of $\zeta_0, \zeta_1, \dots, \zeta_{N-1}$ and the others are independent vectors of $\zeta_0, \zeta_1, \dots, \zeta_{N-1}$, where $r_1 > r_s > r_k$, let ζ_{N-r_s} and $\zeta_{N-r_s-r_k}$ be expressed by

$$\zeta_{N-r_s} = a_0\zeta_0 + a_1\zeta_{r_s} + a_2\zeta_{2\cdot r_s} + \dots + a_{(2^s-2)}\zeta_{(2^s-2)r_s} \qquad (5.5)$$

(cf. Theorem 5.7) and

$$\zeta_{N-r_s-r_k} = b_0\zeta_0 + b_1\zeta_{r_k} + b_2\zeta_{2\cdot r_k} + \dots + b_{N-r_s-2r_k/r_k}\zeta_{N-r_s-2r_k} \qquad (5.6)$$

(cf. Theorem 5.8). Then

$$|a_i| = 1 \qquad \text{for any } i \qquad (0 \le i \le (2^s - s))$$

$$|b_i| = 1 \qquad \text{for any } i \qquad \left(0 \le i \le \frac{N - r_s - 2r_k}{r_k}\right)$$

Proof. From the assumption of this theorem, ζ_i for $N - r_s - r_k \leq i \leq N - 1$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$. Therefore, of course, ζ_i for $N - r_s \leq i \leq N - 1$ is a dependent vector. Therefore, from Theorem 5.7, Eq. (5.5) holds.

From Eq. (5.5),

$$(\zeta_{N-r_s}) \boxtimes (\zeta_{N-r_s}) = a_0\zeta_{N-s} + a_1\zeta_{r_s \oplus (N-r_s)} + \cdots$$

accordingly,

$$\zeta_0 = a_0\zeta_{N-r_s} + a_1\zeta_{r_s \oplus (N-r_s)} + \cdots \qquad (5.7)$$

Substituting ζ_{N-r_s} of Eq. (5.5) to Eq. (5.7),

$$\zeta_0 = a_0\{a_0\zeta_0 + a_1\zeta_{r_s} + \cdots\} + a_1\zeta_{r_s \oplus (N-r_s)} + \cdots = a_0^2\zeta_0 + a_0a_1\zeta_{r_s} + \cdots$$

$$\therefore \quad (a_0^2 - 1)\zeta_0 + a_0a_1\zeta_{r_s} + \cdots = 0 \qquad (5.8)$$

can be obtained.

In Eq. (5.8), the subscript of each ζ in each term of Eq. (5.8) consists of $r_s, 2r_s, \ldots, (2^s - 1)r_s$ since $i \cdot r_s \oplus (N - r_s) < N - r_s$ for $1 \leq i \leq (2^s - 2)r_s$. Therefore, from the assumption, those ζ are independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$. Therefore, in order to let Eq. (5.8) hold, each coefficient must become zero. Therefore,

$$a_0^2 = 1$$

Similarly

$$a_i^2 = 1$$

can be obtained. And, similarly,

$$b_i^2 = 1$$

can be obtained.

6. SOME PROPERTIES OF Z (CF. DEFINITION 3.6)

Suppose the following:

Condition 6.1. The independent vectors of $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{N-1}$ are only $\zeta_0, \zeta_1, \ldots, \zeta_{2^{(k-1)}}, \zeta_{2^{(k-1)}+1}, \ldots, \zeta_{2^{(k-1)}+\ell}$; and ζ_i for any i $(2^{k-1} + \ell + 1 \le i \le N - 1)$ is a dependent vector of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$, where $0 \le \ell \le 2^{(k-1)} - 1$.

Define $V_0, V_1, V_2, \ldots, V_{2^{(n-k)}-1}$ as follows:

$$\left.\begin{array}{lllll}
V_0 & \equiv (\zeta_0, & \zeta_1, & \ldots, & \zeta_{2^k-1}) \\
V_1 & \equiv (\zeta_{2^k}, & \zeta_{2^k+1}, & \ldots, & \zeta_{2^{(k+1)}-1} \\
V_2 & \equiv (\zeta_{2\cdot 2^k}, & \zeta_{2\cdot 2^k+1}, & \ldots, & \zeta_{3\cdot 2^k-1} \\
\vdots & & & & \\
V_{2^{(n-k)}-1} & \equiv (\zeta_{(2^{(n-k)}-1)2^k}, & \zeta_{(2^{(n-k)}-1)2^k}, & \ldots, & \zeta_{N-1})
\end{array}\right\} \quad (6.1)$$

Definition 6.1. Z_i (cf. Definition 3.7)

Define $Z_0, Z_1, Z_2, \ldots, Z_{(2^{(n-k)}-1)}$ as follows:

$$Z_i = \begin{pmatrix}
z_{i2^k}, & z_{i\cdot 2^k+1}, & \ldots, & z_{(i+1)2^k-1} \\
z_{i2^k+1}, & \ldots & & \\
z_{i2^k\oplus j}, & z_{(i\cdot 2^i+1)\oplus j}, & \ldots, & z_{\{(i+1)2^k-1\}\oplus j} \\
z_{(i+1)2^k-1}, & \ldots, & & z_{i2^k}
\end{pmatrix}$$

Accordingly,

$$Z = \begin{pmatrix} Z_0, & Z_1, & Z_2, & \dots, & Z_{(2^{(n-k)}-1)} \\ Z_1, & Z_0, & Z_3, & \dots, & Z_{1\oplus(2^{(n-k)}-1)} \\ \vdots & & & & \\ Z_i & Z_{i\oplus 1}, & Z_{i\oplus 2}, & \dots, & Z_{i\oplus(2^{(n-k)}-1)} \\ \vdots & & & & \\ Z_{(2^{(n-k)}-1)}, & \dots, & & & Z_0 \end{pmatrix}$$

Theorem 6.1. Under Condition 6.1,

$$Z_0^2 = Z_1^2 = \dots = Z^2_{\{2^{(n-k)}-1\}} = \frac{2^k}{\sqrt{N}} Z_0$$

$$Z_i \cdot Z_j = \frac{2^k}{\sqrt{N}} Z_{i\oplus j}$$

holds, where of course $0 \leq i, j \leq \{2^{(n-k)}-1\}$.

Proof. Since the independent vectors of $\zeta_0, \zeta_1, \dots, \zeta_{N-1}$ are only in V_0 under Condition 6.1,

$$V_0V_0^T = V_1V_1^T = \dots = V_{(2^{(n-k)}-1)}V^T_{(2^{(n-k)}-1)} = 2^kE_m \qquad (6.2)$$

can be obtained (cf. Eq. (3.16)).

The following relations hold clearly from Definition 3.5, Definition 3.7 and Definition 6.1, that is,

$$\left.\begin{aligned}
Z_0 &= \frac{1}{\sqrt{N}} V_i^T V_i \\
Z_1 &= \frac{1}{\sqrt{N}} V_i^T V_{i\oplus 1} &&= \frac{1}{\sqrt{N}} V_{i\oplus 1}^T V_i \\
Z_2 &= \frac{1}{\sqrt{N}} V_i^T V_{i\oplus 2} &&= \frac{1}{\sqrt{N}} V_{i\oplus 2}^T V_i \\
&\vdots \\
Z_{\{2^{(n-k)}-1\}} &= \frac{1}{\sqrt{N}} V_i^T V_{i\oplus\{2^{(n-k)}-1\}} &&= \frac{1}{\sqrt{N}} V_{i\oplus\{2^{(n-k)}-1\}}^T V_i
\end{aligned}\right\} \qquad (6.3)$$

for any i $(0 \le i \le 2^{(n-k)} - 1)$.

Therefore, from Eqs. (6.3),

$$Z_i^2 = \frac{1}{\sqrt{N}} V_i^T V_0 \frac{1}{\sqrt{N}} V_0^T V_i = \frac{1}{N} V_i^T V_0 V_0^T V_i = \frac{1}{N} V_i^T (2^k E_m) V_i \text{ (from Eq. (6.2))}$$

$$= \frac{2^k}{N} \sqrt{N} Z_0 \text{ (from Eqs. (6.3))} = \frac{2^k}{\sqrt{N}} Z_0$$

Therefore,

$$Z_0^2 = Z_1^2 = \dots = Z^2_{2^{(n-k)}-1} = \frac{2^k}{\sqrt{N}} Z_0$$

can be obtained. From Eqs. (6.3),

$$Z_i Z_j = \frac{1}{\sqrt{N}} V_i^T V_0 \frac{1}{\sqrt{N}} V_0^T V_j = \frac{1}{N} V_i^T V_0 V_0^T V_j$$

$$= \frac{1}{N} V_i^T (2^k E_m) V_j \text{ (from Eq. (6.2))} = \frac{2^k}{N} V_i^T V_j$$

$$= \frac{2^k}{N} \sqrt{N} Z_{i\oplus j} \text{ (from Eqs. (6.3))} = \frac{2^k}{\sqrt{N}} Z_{i\oplus j}$$

can be obtained.

Theorem 6.2. Under Condition 6.1, any V_i for $1 \leq i \leq \{2^{(n-k)} - 1\}$ can be expressed by

$$V_i = V_0 A_i$$

and

$$V_0 = V_0 A_i^2, \quad V_i = V_i A_i^2$$

can be obtained where

$$A_i = \begin{pmatrix} a_0, & a_1, & a_2, \; \ldots, & a_{(2^k-1)} \\ a_1, & a_0, & \ldots, & a_{1\oplus(2^k-1)} \\ \vdots & & & \\ a_j, & a_{j\oplus 1}, & \ldots, & a_{j\oplus(2^k-1)} \\ \vdots & & & \\ a_{(2^k-1)}, & & \ldots, & a_0 \end{pmatrix} = U_k \begin{pmatrix} \alpha_{0i} & & & & \\ & \alpha_{1i} & & 0 & \\ & & \alpha_{2i} & & \\ & 0 & & \ddots & \\ & & & & \alpha_{(2^k-1)i} \end{pmatrix} U_k$$

$$U_k = \frac{1}{\sqrt{2^k}} \underbrace{\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix} \times \ldots \times \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}}$$

(The number of $\begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix}$ is k.)

Proof. Since every column vector, i.e., ζ in V_i is a dependent vector of ζ_0, ζ_1, ..., ζ_{N-1} from Condition 6.1, $\zeta_{i2^k} \in V_i$ can be expressed as a linear combination of ζ_0, ζ_1, ..., ζ_{2^k-1}, i.e.,

$$\zeta_{i2^k} = a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2^k-1}\zeta_{2^k-1} \tag{6.4}$$

Therefore,

$$(\zeta_{i2^k}) \boxtimes \zeta_j = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2^k-1}\zeta_{2^k-1}) \boxtimes \zeta_j$$

accordingly

$$\zeta_{i2^k+j} = a_0\zeta_j + a_1\zeta_{1\oplus j} + \ldots + a_{2^k-1}\zeta_{(2^k-1)\oplus j} \qquad (6.5)$$

can be obtained for any j $(0 \leq j \leq 2^k - 1)$, where the right-hand side of (6.5) is a linear combination of $\zeta_0, \zeta_1, \ldots, \zeta_{2^k-1}$. Therefore,

$$(\zeta_{i2^k}, \zeta_{i2^k+1}, \ldots, \zeta_{i2^k+(2^k-1)}) = (\zeta_0, \zeta_1, \ldots, \zeta_{2^k-1}) \begin{pmatrix} a_0, & a_1, & a_2, \ldots, & a_{2^k-1} \\ a_1, & a_0, & \ldots, & a_{1\oplus(2^k-1)} \\ \vdots & & & \\ a_{2^k-1}, & a_{2^k-2}, & \ldots, & a_0 \end{pmatrix}$$

Accordingly,

$$V_i = V_0 A_i \qquad (6.6)$$

can be obtained.

Applying Theorem 2.1 to A_i,

$$A_i = U_k \Lambda_i U_k$$

can be obtained.

From Eq. (6.4),

$$(\zeta_{i2^k}) \boxtimes \zeta_{2^k} = (a_0\zeta_0 + a_1\zeta_1 + \ldots + a_{2^k-1}\zeta_{2^k-1}) \boxtimes \zeta_{2^k}$$

Accordingly,

$$\zeta_i = a_0\zeta_{2^k} + a_1\zeta_{2^k+1} + \ldots + a_{2^k-1}\zeta_{2^k+(2^k-1)}$$

can be obtained. Therefore, similarly,

$$(\zeta_0, \zeta_1, \ldots, \zeta_{2^k-1}) = (\zeta_{2^k}, \zeta_{2^k+1}, \ldots, \zeta_{2^{(k+1)}-1})A_i$$

$$\therefore \quad V_0 = V_i A_i \tag{6.7}$$

can be obtained. Therefore, from Eq. (6.6) and Eq. (6.7),

$$V_i = V_i A_i^2$$

and

$$V_0 = V_0 A_i^2$$

can be obtained.

Theorem 6.3. Under Condition 6.1, every V_i for $1 \leq i \leq (2^{(n-k)} - 1)$ can be expressed by

$$V_i = V_0 A_i$$

from Theorem 6.2. Then,

$$A_{i \oplus j} = A_i \cdot A_j$$

can be obtained.

Proof. Since

$$\left.\begin{aligned} V_i &= V_0 A_i \\ V_j &= V_0 A_j \\ V_{i\oplus j} &= V_0 A_{i\oplus j} \end{aligned}\right\} \qquad (6.8)$$

$$V_0^T V_i = V_0^T V_0 A_i$$

$$V_0^T V_j = V_0^T V_0 A_j$$

can be obtained. Therefore, from Eqs. (6.3),

$$\left.\begin{aligned} Z_i &= Z_0 A_i \\ Z_j &= Z_0 A_j \end{aligned}\right\} \qquad (6.9)$$

can be obtained. From Eqs. (6.9) and Theorem 6.1,

$$\begin{aligned} Z_{i\oplus j} &= \frac{\sqrt{N}}{2^k} Z_i Z_j = \frac{\sqrt{N}}{2^k} Z_0 A_i Z_0 A_j = \frac{\sqrt{N}}{2^k} U_k \Lambda_{Z_0} U_k U_k \Lambda_i U_k U_k \Lambda_{Z_0} U_k U_k \Lambda_j U_k \\ &= \frac{\sqrt{N}}{2^k} U_k \Lambda_{Z_0} \Lambda_i \Lambda_j \Lambda_{Z_0} U_k = \frac{\sqrt{N}}{2^k} U_k \Lambda_{Z_0}^2 \Lambda_i \Lambda_j U_k = \frac{\sqrt{N}}{2^k} Z_0^2 A_i A_j = Z_0 A_i A_j \end{aligned} \qquad (6.10)$$

where

$$Z_0 = U_k \Lambda_{Z_0} U_k$$

$$A_i = U_k \Lambda_i U_k$$

$$A_j = U_k \Lambda_j U_k$$

$$\therefore \quad V_0^T V_{i\oplus j} = V_0^T V_0 A_i A_j$$

$$\therefore \quad V_O V_O^T V_{i\oplus j} = V_O V_O^T V_O A_i A_j$$

$$\therefore \quad 2^k E_m V_{i\oplus j} = 2^k E_m V_o A_i A_j \quad \text{(from Eq. (6.2))}$$

$$\therefore \quad V_{i\oplus j} = V_O A_i A_j \tag{6.11}$$

can be obtained. Then from Eq. (6.8) and Eq. (6.11), put

$$A_{i\oplus j} = A_i \cdot A_j$$

Theorem 6.4. Under Condition 6.1,

$$\alpha_{ji} = 1 \text{ or } -1 \text{ or } 0$$

can be obtained, where

$$V_i = V_O A_i \qquad \text{for any } i \qquad (1 \leq i \leq 2^{(n-k)} - 1)$$

$$A_i = U_k \begin{pmatrix} \alpha_{0i} & & & 0 \\ & \alpha_{1i} & & \\ & & \ddots & \\ 0 & & & \alpha_{(2^k-1)i} \end{pmatrix} U_k$$

Without loss of generality, put

$$\alpha_{ji} = 1 \text{ or } -1$$

Accordingly,

$$A_1^2 = A_2^2 = \dots + A^2_{\{2^{(n-k)}-1\}} = E_k$$

Proof. From Theorem 6.2,

$$V_0 = V_0 A_i^2$$

Accordingly,

$$V_0^T V_0 = V_0^T V_0 A_i^2$$

$$\therefore \quad Z_0 = Z_0 A_i^2 \qquad \text{(from Eqs. (6.3))} \tag{6.12}$$

can be obtained.

Let Z_0, A_i be

$$\left.\begin{aligned} Z_0 &= U_k \begin{pmatrix} \nu_0 & & & 0 \\ & \nu_1 & & \\ & & \ddots & \\ 0 & & & \nu_{2^k-1} \end{pmatrix} U_k \\ &\text{and} \\ A_i &= U_k \begin{pmatrix} \alpha_{0i} & & & 0 \\ & \alpha_{1i} & & \\ & & \ddots & \\ 0 & & & \alpha_{(2^k-1)i} \end{pmatrix} U_k \end{aligned}\right\} \tag{6.13}$$

From (6.12) and (6.13),

$$\nu_j = \nu_j \alpha_{ji}^2$$

$$\therefore \quad \nu_j(\alpha_{ji}^2 - 1) = 0 \tag{6.14}$$

can be obtained. From (6.14),

$$\nu_j = 0 \quad \text{or} \quad \alpha_{ji}^2 = 1 \qquad \therefore \quad \alpha_{ji} = \pm 1 \tag{6.15}$$

can be obtained.

Therefore, from Eq. (6.15) and the relation of Theorem 6.1, i.e.,

$$Z_0^2 = Z_1^2 = \ldots = Z^2_{\{2^{(n-k)}-1\}} = \frac{2^k}{\sqrt{N}} Z_0$$

$\alpha_{ji}^2 = 1$ can be determined without loss of generality for any value of ν_j.

Theorem 6.5. The absolute value of characteristic values of Z_i for any i $(0 \leq i \leq 2^{(n-k)} - 1)$ is equal to 0 or $\frac{2^k}{\sqrt{N}}$.

Proof. Applying Theorem 2.1 to Z_0,

$$Z_0 = U_k \begin{pmatrix} \nu_0 & & & 0 \\ & \nu_1 & & \\ & & \ddots & \\ 0 & & & \nu_{2^k-1} \end{pmatrix} U_k$$

can be obtained.

Since

$$Z_0^2 = \frac{2^k}{\sqrt{N}} Z_0$$

holds from Theorem 6.1,

$$\nu_i^2 = \frac{2^k}{\sqrt{N}} \nu_i$$

$$\therefore \quad \nu_i(\nu_i - \frac{2^k}{\sqrt{N}}) = 0$$

$$\therefore \quad \nu_i = 0 \quad \text{or} \quad \nu_i = \frac{2^k}{\sqrt{N}}$$

can be obtained.

Therefore, since

$$Z_0^2 = Z_1^2 = \ldots = Z^2_{\{2^{(n-k)}-1\}} = \frac{2^k}{\sqrt{N}} Z_0$$

holds from Theorem 6.1, the absolute value of characteristic values of Z_i for any i $(0 \leq i \leq 2^{(n-k)} - 1)$ is equal to 0 or $\frac{2^k}{\sqrt{N}}$.

Theorem 6.6. When

$$V_j = V_0 A_j = V_0 U_k \begin{pmatrix} \alpha_{0j} & & & 0 \\ & \alpha_{1j} & & \\ & & \ddots & \\ 0 & & & \alpha_{(2^k-1)j} \end{pmatrix} U_k$$

for any j $(1 \leq j \leq 2^{(n-k)} - 1)$ under Condition 6.1, if

$$\left.\begin{array}{l} \left(u_I^{(n)}\right)^T \in V \\ \\ \text{and} \\ \\ I = S2^k + i \end{array}\right\}$$

holds, where $0 \leq S \leq 2^{(n-k)} - 1$ and $0 \leq i \leq (2^k - 1)$,

$$(1,\alpha_{i1},\alpha_{i2},\ldots,\alpha_{i(2^{(n-k)}-1)}) = \left(\xi_S^{(n-k)}\right)^T$$

holds where

$$U_n = \left(u_0^{(n)},u_1^{(n)},\ldots,u_{N-1}^{(n)}\right) = \frac{1}{\sqrt{N}}\left(\xi_0^{(n)},\xi_1^{(n)},\ldots,\xi_{N-1}^{(n)}\right)$$

cf. Definition 3.5.

Proof. Since

$$\left(u_I^{(n)}\right)^T \in V$$

$$I = S2^k + i$$

holds from the assumption

$$\left(u_I^{(n)}\right)^T = \left(u_i^{(k)},u_i^{(k)},\ldots,u_i^{(k)}\right) \otimes \left(\xi_S^{(n-k)}\right)^T \qquad (6.16)$$

can clearly be obtained. Therefore,

$$V_0 \in \left(u_i^{(k)}\right)^T$$

holds.

Let the ith row vector of V_j be v_i.

Since

$$V_j = V_0 A_j$$

$$v_i = \left(u_i^{(k)}\right)^T A_j$$

can be obtained. Therefore, from Theorem 2.2,

$$v_i = \left(u_i^{(k)}\right)^T A_j = \alpha_{ij} \left(u_i^{(k)}\right)^T$$

can be obtained. Therefore,

$$\left(u_I^{(n)}\right)^T = \left(u_i^{(k)^T}, \alpha_{i1} u_i^{(k)^T}, \alpha_{i2} u_i^{(k)^T}, \ldots, \alpha_{i(2^{(n-k)}-1)} u_i^{(k)^T}\right)$$

$$= \left(u_i^{(k)^T}, u_i^{(k)^T}, \ldots, u_i^{(k)^T}\right) \boxtimes \left(1, \alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{i(2^{(n-k)}-1)}\right) \tag{6.17}$$

can be obtained. Therefore, from Eq. (6.16) and Eq. (6.17),

$$\left(1, \alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{i(2^{(n-k)}-1)}\right) = \left(\xi_S^{(n-k)}\right)^T$$

can be obtained.

Condition 6.2. Suppose that there exists $\xi_i^{(k)}$ for a suitable i $(0 \leq i \leq 2^k - 1)$ corresponding to A_j for any j $(1 \leq j \leq 2^{(n-k)} - 1)$ such that

$$\xi_i^{(k)} = \begin{pmatrix} \alpha_{0j} \\ \alpha_{1j} \\ \alpha_{2j} \\ \vdots \\ \alpha_{(2^k-1)j} \end{pmatrix}$$

where

$$A_j = U_k \begin{pmatrix} \alpha_{0j} & & & & \\ & \alpha_{1j} & & 0 & \\ & & \alpha_{2j} & & \\ & & & \ddots & \\ & 0 & & & \alpha_{(2^k-1)j} \end{pmatrix} U_k$$

(cf. Theorem 6.2).

<u>Theorem 6.7</u>. Let A_j be

$$A_j = \begin{pmatrix} a_0, & a_1, & a_2, & \ldots, & a_{(2^k-1)} \\ a_1, & a_0, & a_3, & \ldots, & a_{1\oplus(2^k-1)} \\ \vdots & & & & \\ a_\ell, & a_{\ell\oplus 1}, & a_{\ell\oplus 2}, & \ldots, & a_{\ell\oplus(2^k-1)} \\ \vdots & & & & \\ a_{(2^k-1)}, & & & \ldots, & a_0 \end{pmatrix}$$

Under Condition 6.2,

$$a_0 = a_1 = \ldots = a_{i-1} = a_{i+1} = \ldots = a_{(2^k-1)} = 0$$

and

$$a_i = 1$$

can be obtained.

Proof. Applying Theorem 2.1 to A_j

$$a_\ell = \frac{1}{\sqrt{2^k}} (\alpha_{j0}, \alpha_{j1}, \ldots, \alpha_{j(2^k-1)}) u_\ell^{(k)} = \frac{1}{\sqrt{2^k}} \left(\xi_i^{(k)}\right)^T u_\ell^{(k)} = \left(u_i^{(k)}\right)^T u_\ell^{(k)}$$

can be obtained. Therefore,

$$a_\ell = 1 \qquad \text{when } \ell = i \quad ,$$
$$a_\ell = 0 \qquad \text{when } \ell \neq i$$

can be obtained.

Now, in the case of a group code, it is found below that Condition 6.1 and Condition 6.2 are satisfied.

In a group code, if there exist row vectors of V in $u_0^{(n)^T}$, $u_1^{(n)^T}$, ..., $u_{2^{(n-1)}-1}^{(n)^T}$ and in $u_{2^{(n-1)}}^{(n)^T}$, $u_{2^{(n-1)}+1}^{(n)^T}$, ..., $u_{N-1}^{(n)^T}$, the number of row vectors of V in $u_0^{(n)^T}$, $u_1^{(n)^T}$, ..., $u_{2^{(n-1)}-1}^{(n)^T}$ is equal to the number of row vectors of V in $u_{2^{(n-1)}}^{(n)^T}$, $u_{2^{(n-1)}+1}^{(n)^T}$, ..., $u_{N-1}^{(n)^T}$.

Similarly, in a group code, if there exist row vectors V in $u_0^{(n)^T}$, $u_1^{(n)^T}$, ..., $u_{2^k-1}^{(n)^T}$ and in $u_{2^k}^{(n)^T}$, $u_{2^k+1}^{(n)^T}$, ..., $u_{2^{(k+1)}-1}^{(n)^T}$, the number of row vectors of V in $u_0^{(n)^T}$, $u_1^{(n)^T}$, ..., $u_{2^k-1}^{(n)^T}$ is equal to the number of row vectors of V in $u_{2^k}^{(n)^T}$, $u_{2^k+1}^{(n)^T}$, ..., $u_{2^{(k+1)}-1}^{(n)^T}$. Therefore, if there exist any independent vectors of ζ_0, ζ_1, ..., ζ_{N-1} in $\zeta_{\ell 2^k}$, $\zeta_{\ell 2^k+1}$, ..., $\zeta_{(\ell+1)2^k-1}$ and in $\zeta_{(\ell+1)2^k}$, $\zeta_{(\ell+1)2^k+1}$, ..., $\zeta_{(\ell+2)2^k-1}$, the number of independent vectors of ζ_0, ζ_1, ..., ζ_{N-1} in $\zeta_{\ell 2^k}$, $\zeta_{\ell 2^k+1}$, ..., $\zeta_{(\ell+1)2^k-1}$ is equal to the number of independent vectors of ζ_0, ζ_1, ..., ζ_{N-1} in $\zeta_{(\ell+1)2^k}$, $\zeta_{(\ell+1)2^k+1}$, ..., $\zeta_{(\ell+2)2^k-1}$.

Therefore, since the total number of group codes is of the form 2^s, if there exist independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ in $\zeta_0, \zeta_1, \ldots, \zeta_{2^k-1}$, the number of independent vectors is of the form 2^t $(t \leq s)$. Therefore, applying Theorem 5.10 a suitable number of times to $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ and renumbering the subscripts in natural order from the first vector, only $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{(2^s-1)}$ are independent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ and the others are dependent vectors of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$. This is Condition 6.1.

Now, consider $u_{I_a}^{(n)^T}, u_{I_b}^{(n)^T}, u_{I_c}^{(n)^T} \in V$ where

$$\left.\begin{aligned} I_a &= S_a 2^s + a \\ I_b &= S_b 2^s + b \\ I_c &= S_c 2^s + c \end{aligned}\right\} \qquad (6.18)$$

and $0 \leq S_a, S_b, S_c \leq (2^{(n-s)} - 1)$, $0 \leq a, b, c \leq (2^s - 1)$.

Assume that

$$I_a \oplus I_b = I_c \qquad (6.19)$$

holds. (There always exists I_c such that $I_a \oplus I_b = I_c$ is a group code.)

Therefore, from Eq. (6.18) and Eq. (6.19),

$$S_c 2^s + c = (S_a \oplus S_b)2^b + (a \oplus b)$$

$$\therefore \quad \left.\begin{aligned} S_c &= S_a \oplus S_b \\ c &= a \oplus b \end{aligned}\right\} \qquad (6.20)$$

can be obtained.

Applying Theorem 6.6 to Eq. 6.20,

$$\xi^{(n-s)}_{S_c} < \xi^{(n-s)}_{S_a \oplus S_b} = \xi^{(n-s)}_{S_a} \boxtimes \xi^{(n-s)}_{S_b} \tag{6.21}$$

can be obtained.

Now, $u_0^{(n)} \in V$ can be assumed without loss of generality. Therefore, Eq. (6.21) means that Condition 6.2 is satisfied.

Remark 6.1. In the case that Condition 6.1 and Condition 6.2 are satisfied but the code is not a group code,

$$S_c = S_a \oplus S_b$$

is satisfied but

$$c \neq a \oplus b$$

holds (cf. Eq. (6.20).

Remark 6.2. When V satisifes Condition 6.1 and Condition 6.2, and

$$\xi_i^{(k)} = \begin{pmatrix} \alpha_{0j} \\ \alpha_{1j} \\ \alpha_{2j} \\ \vdots \\ \alpha_{(2^k-1)j} \end{pmatrix}$$

holds (cf. Condition 6.2),

$$\{\alpha_{0j}, \alpha_{1n}, \alpha_{2j}, \ldots, \alpha_{(2^k-1)j}\}$$

becomes an Abelian group under the operation of multiplication. Accordingly, considering the matrix α

$$\alpha = \begin{pmatrix} 1, & 1, & 1, & 1, & \ldots, & 1 \\ 1, & \alpha_{11}, & \alpha_{12}, & \alpha_{13}, & \ldots, & \alpha_{1(2^{n-k})-1)} \\ 1, & \alpha_{21}, & \alpha_{22}, & \alpha_{23}, & \ldots, & \alpha_{2(2^{(n-k)}-1)} \\ \vdots & & & & & \\ 1, & \alpha_{(2^k-1)1}, & \alpha_{(2^k-1)2}, & & \ldots, & \alpha_{(2^k-1)(2^{(n-k)}-1)} \end{pmatrix}$$

(as $u_0^{(n)} \in V$ can be assumed without loss of generality, it may follow that $\alpha_{01} = \alpha_{02} = \ldots = \alpha_{0(2^{(n-k)}-1)} = 1$) there exist $i_1, i_2, \ldots, i_{\{2^{(n-k)}-1\}}$ such that

$$\alpha = \left(\xi_0^{(k)}, \xi_{i_1}^{(k)}, \xi_{i_2}^{(k)}, \ldots, \xi_{i_{\{2^{(n-k)}-1\}}}^{(k)}\right)$$

from Condition 6.2.

From Theorem 6.6 and Condition 6.2, α is reduced to the following form:

$$\alpha = \begin{pmatrix} \xi_0^{(n-k)^T} \\ \xi_{S_1}^{(n-k)^T} \\ \xi_{S_2}^{(n-k)^T} \\ \vdots \\ \xi_{S_{2^k-1}}^{(n-k)^T} \end{pmatrix} \qquad (6.22)$$

Since $\{1,\alpha_{ij},\alpha_{2j},\ldots,\alpha_{(2^k-1)j}\}$ is an Abelian group as mentioned above,

$$\left\{\xi_0^{(n-k)},\xi_{S_1}^{(n-k)},\ldots,\xi_{S_{2^k-1}}^{(n-k)}\right\}$$

becomes an Abelian group under the operation "$\boxtimes$".

7. SOLUTION OF EQ. (3.25) "$V\Lambda' V^T = 0$" UNDER CONDITION 6.1 and CONDITION 6.2

Even if generators of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ are rearranged in any order, Eq. (3.25), i.e., $V\Lambda' V^T = 0$, holds. Let the transformation of the rearrangement of generators of $\zeta_0, \zeta_1, \ldots, \zeta_{N-1}$ be τ, that is,

$$V'\tau = W$$

From Theorem 4.4, Λ' is invariant under the transformation, i.e.,

$$\tau\Lambda'\tau^T = \Lambda'$$

Therefore,

$$W\Lambda' W^T = V\tau\Lambda'\tau^T V^T = V\Lambda' V^T = 0 \tag{7.1}$$

can be obtained.

Since it is clear that $A_i^T = A_i$ holds from Theorem 6.3,

$$V\Lambda' V^T = (V_0, V_0A_1, V_0A_2, \ldots, V_0A_{\{2^{(n-k)}-1\}})\Lambda'(V_0, V_0A_1, \ldots, V_0A_{\{2^{(n-k)}-1\}})^T$$

$$= V_0(\Lambda_0 + A_1\Lambda_1A_1 + A_2\Lambda_2A_2 + \ldots + A_{\{2^{(n-k)}-1\}}\Lambda_{\{2^{(n-k)}-1\}}A_{\{2^{(n-k)}-1\}})V_0^T = 0$$

Accordingly,

$$V_0(\Lambda_0 + A_1\Lambda_1A_1 + A_2\Lambda_2A_2 + \ldots + A_{\{2^{(n-k)}-1\}}\Lambda_{\{2^{(n-k)}-1\}}A_{\{2^{(n-k)}-1\}})V_0^T = 0 \tag{7.2}$$

can be obtained, where

$$\Lambda' \equiv \begin{pmatrix} \Lambda_0 & & & 0 \\ & \Lambda_1 & & \\ & & \ddots & \\ 0 & & & \Lambda_{\{2^{(n-k)}-1\}} \end{pmatrix} \tag{7.3}$$

Considering Theorem 6.7, let A_j for any j $(1 \leq j \leq 2^{(n-k)} - 1)$ be

$$\left.\begin{aligned} A_j &= \begin{pmatrix} a_0, & a_1, & \ldots, & a_{2^k-1} \\ \vdots & & & \\ a_i, & a_{i\oplus 1}, & \ldots, & a_{i\oplus(2^k-1)} \\ \vdots & & & \\ a_{2^k-1}, & & \ldots, & a_0 \end{pmatrix} \\ a_0 = a_1 = \ldots &= a_{i_j-1} = a_{i_j+1} = \ldots = a_{2^k-1} = 0 \\ a_{i_j} &= 1 \end{aligned}\right\} \tag{7.4}$$

where

$$0 \leq i_j \leq 2^k - 1 \tag{7.5}$$

Since

$$\Lambda_j = \begin{pmatrix} \lambda'_{j2^k} & & & 0 \\ & \lambda'_{j2^k+1} & & \\ & & \ddots & \\ 0 & & & \lambda'_{j2^k+2^k-1} \end{pmatrix}$$

holds from Eq. (7.3),

$$A_j\Lambda_jA_j = \begin{pmatrix} \lambda'_{j2^k+i_j} & & & 0 \\ & \lambda'_{j2^k+(1\oplus i_j)} & & \\ & & \ddots & \\ 0 & & & \lambda'_{[j2^k+\{2^k-1)\oplus i_j\}]} \end{pmatrix} \qquad (7.6)$$

can be obtained from Eq. (7.4).

Therefore, let

$$\Lambda_0 + A_1\Lambda A_1 + \ldots + A_{\{2^{(n-k)}-1\}}\Lambda_{\{2^{(n-k)}-1\}}A_{\{2^{(n-k)}-1\}} = \begin{pmatrix} \nu_0 & & & 0 \\ & \nu_1 & & \\ & & \ddots & \\ 0 & & & \nu_{(2^k-1)} \end{pmatrix}$$

(7.7)

The following relations can be obtained:

$$\nu_0 = \lambda'_0 + \lambda'_{2^k+i_1} + \lambda'_{2\cdot 2^k+i_2} + \lambda'_{3\cdot 2^k+i_3} + \ldots + \lambda'_{\{2^{(n-k)}-1\}2^k+i_{\{2^{(n-k)}-1\}}}$$

In general,

$$\nu_j = \lambda'_j + \lambda'_{2^k+(j\oplus i_1)} + \lambda'_{2\cdot 2^k+(j\oplus i_2)} + \ldots + \lambda'_{\{2^{(n-k)}-1\}2^k+\{j\oplus i_{\{2^{(n-k)}-1\}}\}}$$

where

$$0 \leq j \leq (2^k - 1)$$

(7.8)

Now, the solution such that the number of most efficient codes is 2^k is discussed below.

Theorem 7.1. In Eq. (7.8), when $\nu_0 = 0$,

$$\nu_j = 0$$

can be obtained for any j $(0 \leq j \leq (2^k - 1))$.

Proof. Applying the result of Theorem 3.1 to Eq. (7.8),

$$\begin{aligned}\nu_0 &= \lambda'_0 + \lambda'_{2^k+i_1} + \dots + \lambda'_{\{2^{(n-k)}-1\}2^k+i_{\{2^{(n-k)}-1\}}} \\ &= (h'_0, h_1, \dots, h_{N-1})\left(u_0^{(n)} + u^{(n)}_{2^k+i_1} + \dots + u^{(n)}_{\{2^{(n-k)}-1\}2^k+i_{\{2^{(n-k)}-1\}}}\right)\end{aligned} \qquad (7.9)$$

can be obtained, where $h'_0 = h_0 - 1 = 0$.

Since

$$\alpha = \left(\xi_0^{(k)}, \xi_{i_1}^{(k)}, \dots, \xi^{(k)}_{i_{\{2^{(n-k)}-1\}}}\right)$$

is an Abelian group from Remark 6.2 whose generators (i.e., bases of the Abelian group) are $\xi_0^{(k)}$, $\xi_{i_1}^{(k)}$, $\xi_{i_2}^{(k)}$, $\xi_{i_{2^2}}^{(k)}$, ..., $\xi^{(k)}_{2^{(n-k-1)}}$,

$$\begin{aligned}&u_0^{(n)} + u^{(n)}_{2^k+i_1} + \dots + u^{(n)}_{\{2^{(n-k)}-1\}2^k+i_{\{2^{(n-k)}-1\}}} \qquad (7.10) \\ &= \left(u_0^{(n)} + u^{(n)}_{2^k+i_1}\right) \boxtimes \left(u_0^{(n)} + u_{2^{(k+1)}+i_2}\right) \boxtimes \left(u_0^{(n)} + u^{(n)}_{2^{(k+2)}+i_{2^2}}\right) \boxtimes \dots \\ &\qquad \boxtimes \left(u_0^{(n)} + u_{2^{(n-k-1)}+i_{(n-k-1)}}\right)\end{aligned}$$

can be obtained.

Since $u_i^{(n)}$ is the column vector of U_n, the elements of $\left(u_0^{(n)} + u_i^{(n)}\right)$ are 0 or 2, i.e., non-negative in general. Therefore, letting

$$\text{the right-hand side of Eq. (7.10)} \equiv \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{pmatrix} \tag{7.11}$$

$$x_i \geq 0 \tag{7.12}$$

can be obtained for any i $(0 \leq i \leq (N - 1))$.

From Eq. (7.9) and Eq. (7.11),

$$\nu_0 = (h_0', h_1, \ldots, h_{N-1}) \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} = h_0' x_0 + h_1 x_1 + \ldots + h_{N-1} x_{N-1} \tag{7.13}$$

can be obtained.

Therefore, when $\nu_0 = 0$ holds,

$$h_i = 0 \qquad \text{when } x_i \neq 0 \tag{7.14}$$

can be obtained from Definition 3.2, Eqs. (3.5) and (7.12).

Now, from Eq. (7.8),

$$\nu_j = \lambda'_j + \lambda'_{2^k+(j\oplus i_1)} + \dots + \lambda'_{\{2^{(n-k)}-1\}2^k+\{j\oplus i_{\{2^{(n-k)}-1\}}\}}$$

$$= (h'_0, h_1, \dots, h_{N-1}) \left(u_j^{(n)} + u^{(n)}_{2^k+(j\oplus i_1)} + \dots + u^{(n)}_{\{2^{(n-k)}-1\}2^k+\{j\oplus i_{\{2^{(n-k)}-1\}}\}} \right)$$

$$= (h'_0, h_1, \dots, h_{N-1}) \left[\left(u_0^{(n)} + u_{2^k+i_1} + \dots + u_{\{2^{(n-k)}-1\}2^k+i_{\{2^{(n-k)}-1\}}} \right) \boxtimes u_j^{(n)} \right]$$

$$= (h'_0, h_1, \dots, h_{N-1}) \left[\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} \boxtimes u_j^{(n)} \right] \qquad \text{(from Eq. 7.10) and Eq. (7.11)}$$

$$= (h'_0, h_1, \dots, h_{N-1}) \begin{pmatrix} x_0 u_{0j} \\ x_1 u_{1j} \\ \vdots \\ x_{N-1} u_{(N-1)j} \end{pmatrix}$$

$$= h'_0 x_0 u_{0j} + h_1 x_1 u_{1j} + \dots + h_{(N-1)} x_{(N-1)} u_{(N-1)j}$$

$$= 0 \qquad \text{(from Eq. (7.14))}$$

can be obtained.

Now, in the solution of $V\Lambda'V = 0$ such that the number of most efficient codes is 2^k,

$$\det V_0 \neq 0$$

can be obtained. Therefore, from Eq. (7.2),

$$\Lambda_0 + A_1\Lambda_1A_1 + A_2\Lambda_2A_2 + \dots + A_{\{2^{(n-k)}-1\}}\Lambda_{\{2^{(n-k)}-1\}}A_{\{2^{(n-k)}-1\}} = 0 \tag{7.15}$$

can be obtained. Therefore, from Eq. (7.15) and Eq. (7.7),

$$\begin{pmatrix} \nu_0 & & & & \\ & \nu_1 & & 0 & \\ & & \nu_2 & & \\ & & & \ddots & \\ & 0 & & & \nu_{(2^k-1)} \end{pmatrix} = 0 \tag{7.16}$$

can be obtained.

Therefore, the problem can be reduced to that of obtaining maximum k such that Eq. (7.16) holds. Accordingly, from Theorem 7.1 the problem can be reduced to that of obtaining maximum k such that $\nu_0 = 0$.

Theorem 7.2. The problem of obtaining maximum k such that $\nu_0 = 0$ can be reduced to obtaining a solution in non-negative integers x_1, x_2, ..., x_2, k, for the equations

$$\lambda_0 + x_1\lambda'_{r_1} + x_2\lambda'_{(r_1+r_2)} + \dots + x_n\lambda_{(r_1+r_2+\dots+r_n)} = 0 \tag{7.17}$$

$$1 + x_1 + x_2 + \dots + x_n = 2^{(n-k)} \tag{7.18}$$

which maximizes k where

(I) when $k \geq (n - k)$.

$$\left.\begin{aligned}
x_1 &\leq {}_{n-k}C_1 \\
x_1 + x_2 &\leq {}_{n-k}C_1 + {}_{n-k}C_2 \\
&\vdots \\
x_1 + x_2 + \dots + x_{n-k} &\leq {}_{n-k}C_1 + {}_{n-k}C_2 + \dots + {}_{n-k}C_{n-k} = 2^{(n-k)} - 1 \\
x_1 + x_2 + \dots + x_{n-k+1} &\leq 2^{(n-k)} - 1 \\
&\vdots \\
x_1 + x_2 + \dots + x_{k+1} &\leq 2^{(n-k)} - 1 \\
x_2 + x_3 + \dots + x_{k+1} + x_{k+2} &\leq {}_{n-k}C_2 + {}_{n-k}C_3 + \dots + {}_{n-k}C_{n-k} \\
x_3 + \dots + x_{k+2} + x_{k+3} &\leq {}_{n-k}C_3 + {}_{n-k}C_4 + \dots + {}_{n-k}C_{n-k} \\
&\vdots \\
x_{(n-k)} + \dots + x_n &\leq {}_{n-k}C_{n-k}
\end{aligned}\right\} \quad (7.19)$$

(II) when $k < (n - k)$.

$$\left.\begin{array}{r}
x_1 \leq {}_{n-k}C_1 \\
x_1 + x_2 \leq {}_{n-k}C_1 + {}_{n-k}C_2 \\
x_1 + x_2 + x_3 \leq {}_{n-k}C_1 + {}_{n-k}C_2 + {}_{n-k}C_3 \\
\vdots \\
x_1 + x_2 + \cdots + x_{k+1} \leq {}_{n-k}C_1 + {}_{n-k}C_2 + \cdots + {}_{n-k}C_{k+1} \\
x_2 + \cdots + x_{k+1} + x_{k+2} \leq {}_{n-k}C_2 + {}_{n-k}C_3 + \cdots + {}_{n-k}C_{k+2} \\
x_3 + \cdots + x_{k+3} \leq {}_{n-k}C_3 + \cdots + {}_{n-k}C_{k+3} \\
\vdots \\
x_{n-2k} + \cdots + x_{n-k} \leq {}_{n-k}C_{n-2k} + \cdots + {}_{n-k}C_{n-k} \\
x_{n-2k+1} + \cdots + x_{n-k+1} \leq {}_{n-k}C_{n-2k+1} + \cdots + {}_{n-k}C_{n-k} \\
\vdots \\
x_{n-k} + \cdots + x_n \leq {}_{n-k}C_{n-k}
\end{array}\right\} \tag{7.20}$$

and where

$$r_1 = 2^{n-1},\ r_2 = 2^{n-2},\ \ldots,\ r_{n-1} = 2^1,\ r_n = 1$$

and

$$x_1,\ x_2,\ \ldots,\ x_n \text{ are non-negative integers}$$

Remark 7.1. Equation (7.17) is an indefinite equation of n variables $(x_1, x_2, \ldots, x_n)$ of the first order. Therefore, the general solution can be always obtained. First, obtain a solution for maximum k in the general solution such that Eq. (7.18) is satisfied. Then the conditions, i.e., $k \geq n - k$ or $k < n - k$ are determined. Next, investigate whether the solution satisfies Eq. (7.19) or Eq. (7.20) corresponding to the conditions $k \geq n - k$ or $k < n - k$, respectively. If the solution does not satisfy Eq. (7.19) or Eq. (7.20), obtain the solution about the next maximum k in the general solution such that Eq. (7.18) is satisfied.

Continuing the precedure, the solution for maximum k such that Eq. (7.18) and Eq. (7.19) or Eq. (7.20) are satisfied, can be obtained.

This is the desired solution.

Proof of Theorem 7.2. In ν_0 (cf. Eq. (7.8)), since $0 \leq i_1 \leq 2^k - 1$ (cf. Eq. (7.5)), there exists a possibility that $\lambda'_{2^k+i_1} = \lambda'_{r_1}$ or $\lambda'_{r_1+r_2}$, or ..., or $\lambda_{r_1+r_2+\ldots+r_{k+1}}$ (cf. Theorem 4.4). A similar possibility exists with respect to $\lambda_{2^{(k+1)}+i_2}$, $\lambda'_{2^{(k+2)}+i_{2^2}}$, ..., $\lambda'_{2^{(n-1)}+i_{2^{(n-k-1)}}}$. Therefore, the number of λ' having the possibility is ${}_{n-k}C_1$.

Next, there exists a possibility that $\lambda'_{3\cdot 2^k+i_3} = \lambda_{r_1+r_2}$ or $\lambda'_{r_1+r_2+r_3}$ or ..., or $\lambda'_{r_1+r_2+\ldots+r_{k+2}}$. A similar possibility exists with respect to $\lambda'_{5\cdot 2^k+i_5}$, $\lambda_{6\cdot 2^k+i_6}$, ..., and the number of λ' which has the possibility is ${}_{n-k}C_2$.

Continuing the discussion, Fig. 7.1 and Fig. 7.2 can be obtained corresponding to $k \geq n - k$ and $k < n - k$, respectively.

In Fig. 7.1 and Fig. 7.2, (i) and $(i)2^k + j$ mean, respectively, $\lambda'_{r_1+r_2+\ldots+r_i}$ and $\lambda'_{(r_1+r_2+\ldots+r_i)2^k+j}$.

As shown clearly in Fig. 7.1 and Fig. 7.2, the conditions (7.19) and (7.20) can be obtained corresponding to $k \geq n - k$ and $k < n - k$, respectively. Equation (7.17) is also satisfied.

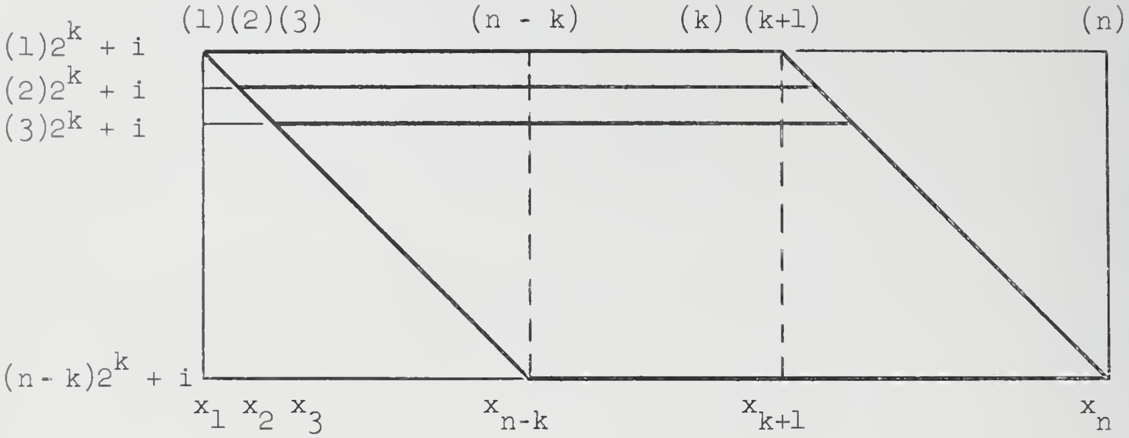


Figure 7.1. $(k \geq (n - k))$

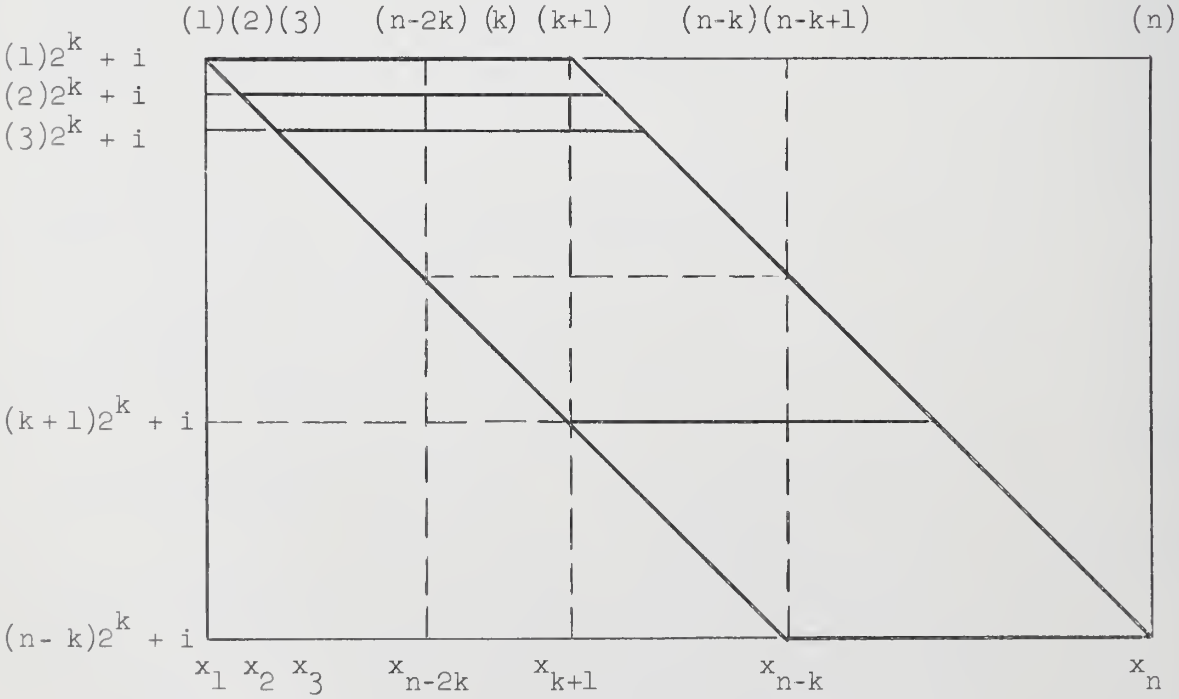


Figure 7.2. $(k < (n - k))$

Since the number of terms of the right-hand side of Eq. (7.8) is $2^{(n-k)}$, it is clear that Eq. (7.18) must hold.

Now, suppose that maximum k and $x_1, x_2, \ldots, x_n$ such that Eq. (7.17), Eq. (7.18) and Eq. (7.19) or Eq. (7.20) are satisfied, have been obtained.

From Eq. (7.19) and Eq. (7.20),

$$x_1 \leq {}_{n-k}C_1$$

holds. Therefore, x_1 of the elements $\lambda'_{2^k+i_1}$, $\lambda'_{2^{k+1}+i_2}$, $\lambda'_{2^{k+2}+i_{2^2}}$, ..., $\lambda'_{2^{(n-1)}+i_{2^{(n-k-1)}}}$, can take the value λ'_{r_1}. It is quite arbitrary which of them take the value λ'_{r_1}.

Therefore, let x_1 of them take the value λ'_{r_1}.

Next, let x_2 of the others whose number is $({}_{n-k}C_1 - x_1)$ and $\lambda'_{3\cdot 2^k+i_3}$, $\lambda'_{5\cdot 2^k+i_5}$, ..., in general $\lambda'_{(2)2^k+i}$ take the value $\lambda'_{r_1+r_2}$. Since

$$x_1 + x_2 \leq {}_{n-k}C_1 + {}_{n-k}C_2$$

holds from Eq. (7.19) and Eq. (7.20), the procedure is always possible.

Continuing such a procedure (it is always possible since Eq. (7.19) and Eq. (7.20) hold corresponding to $k \geq n - k$ and $k < n - k$, respectively and Eq. (7.18) holds), the value of each term of the right-hand side of Eq. (7.8) can be determined and $\nu_0 = 0$ holds from Eq. (7.17). Then, of course, i_1, i_2, i_3, ..., can also be determined.

Remark 7.2. The values of i_1, i_2, ..., can be determined as shown in the proof of Theorem 7.2.

Since

$$V_0 = V_j A_j$$

holds for any j $(0 \leq j \leq 2^{(n-k)} - 1)$ from Eq. (6.7),

$$\zeta_0 = \zeta_{j2^k \oplus i_j} = \zeta_{j2^k + i_j} \tag{7.21}$$

can be obtained from Theorem 6.7.

Therefore, from Eq. (7.21)

$$\left.\begin{aligned}
\zeta_1 &= \zeta_{j2^k+(i_j \oplus 1)} \\
\zeta_2 &= \zeta_{j2^k+(i_j \oplus 2)} \\
&\vdots \\
\zeta_{2^k-1} &= \zeta_{j2^k+\{i_j \oplus (2^k-1)\}}
\end{aligned}\right\} \tag{7.22}$$

can be obtained. Therefore,

$$\left.\begin{aligned}
z_0 &= z_{j2^k+i_j} \\
z_1 &= z_{j2^k+(i_j \oplus 1)} \\
z_2 &= z_{j2^k+(i_j \oplus 2)} \\
&\vdots \\
z_{2^k-1} &= z_{j2^k+\{i_j \oplus (2^k-1)\}}
\end{aligned}\right\} \tag{7.23}$$

can be obtained.

Now, from Theorem 3.1 and Eq. (3.27),

$$Z\Lambda'Z = U_n \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} U_n\Lambda'U_n \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} U_n$$

$$= U_n \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} \{H(n,p) - E_N\} \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} U_n$$

$$= 0$$

Accordingly,

$$\begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} \{H(n,p) - E_N\} \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} = 0 \qquad (7.24)$$

can be obtained.

Equation (7.24) means that when x_i is identically zero, $u_i^{(n)^T} \notin V$ and when x_i is not identically zero, $u_i^{(n)^T} \in V$.

On the other hand, applying (Theorem 2.1) to Z,

$$x_i = \sqrt{N}\,(z_0, z_1, \ldots z_{N-1})u_i^{(n)} \qquad (7.25)$$

can be obtained, for any i $(0 \leq i \leq N - 1)$.

Therefore, it is possible from Eq. (7.23) and Eq. (7.25) to find $u_i^{(n)}$ such that

$$\left.\begin{array}{lll} u_i^{(n)} \in V_i & & \text{when } x_i \not\equiv 0 \\ \\ u_i^{(n)} \notin V_i & & \text{when } x_i \equiv 0 \end{array}\right\} \qquad (7.26)$$

Therefore, all the codes corresponding to the binary expression of i such that $x_i \not\equiv 0$ are the set of most efficient codes under the conditions.

Remark 7.3. In general, $2^1 \leq$ the number of most efficient codes $\leq 2^{n-p+1}$ holds (cf. Y. Komamiya: Bulletin of Electrotechnical Laboratory, Vol. 17, pp. 298-310, 1953 and Proceedings of the Third Japan National Congress for Applied Mechanics, 1954). Therefore, letting K_0 be a maximum k,

$$1 \leq K_0 \leq n - p + 1 \qquad (7.27)$$

can be obtained.

Remark 7.4. When there exist $A_1, A_2, \ldots, A_{\{2^{(n-k)}-1\}}$ satisfying Eq. (7.15), $\pm A_1, \pm A_2 \ldots, \pm A_{\{2^{(n-k)}-1\}}$ also clearly satisfy Eq. (7.15).

Example 7.1. The case of n = 3, p = 2.

From Theorem 4.4 and Theorem 4.6,

$$\lambda_0 = 4$$

$$\lambda_{r_1} = 2$$

$$\lambda_{r_1+r_2} = 0$$

$$\lambda_{r_1+r_2+r_3} = -2$$

Accordingly,

$$\left.\begin{aligned} \lambda'_0 &= 3 \\ \lambda'_{r_1} &= 1 \\ \lambda'_{r_1+r_2} &= -1 \\ \lambda'_{r_1+r_2+r_3} &= -3 \end{aligned}\right\} \qquad (7.28)$$

$$\therefore \quad \left.\begin{aligned} &\lambda'_0 = 3 \\ &\lambda'_1 = \lambda'_2 = \lambda'_4 = 1 \\ &\lambda'_3 = \lambda'_5 = \lambda'_6 = -1 \\ &\lambda'_7 = -3 \end{aligned}\right\} \qquad (7.29)$$

can be obtained.

Applying Theorem 7.2 to this case,

$$\left.\begin{aligned} 3 + x_1 - x_2 - 3x_3 &= 0 \\ 1 + x_1 + x_2 + x_3 &= 2^{(3-k)} \end{aligned}\right\} \qquad (7.30)$$

From Eq. (7.27),

$$k \leq n - p + 1 = 3 - 2 + 1 = 2$$

can be obtained.

Now, let k be 2, i.e.,

$$k = 2 \tag{7.31}$$

Therefore, from Eq. (7.31) and Eqs. (7.30),

$$\left.\begin{aligned} x_1 - x_2 - 3x_3 + 3 &= 0 \\ x_1 + x_2 + x_3 - 1 &= 0 \end{aligned}\right\}$$

$$\therefore \quad \left.\begin{aligned} x_3 &= 1 \\ x_1 = x_2 &= 0 \end{aligned}\right\} \tag{7.32}$$

can be obtained. From Eq. (7.31),

$$k = 2 > n - k = 3 - 2 = 1$$

$$\therefore \quad k > n - k \tag{7.33}$$

can be obtained.

It is shown below that Eqs. (7.32) satisfy Eqs. (7.19):

$$\left.\begin{aligned} x_1 &= 0 \leq {}_2C_1 \\ x_1 &= 0 \leq 2^{n-k} - 1 = 2' - 1 = 1 \\ x_1 + x_2 &= 0 \leq 2' - 1 = 1 \\ x_1 + x_2 + x_3 &= 1 \leq 2' - 1 = 1 \\ x_1 + x_2 + x_3 &= 1 \leq {}_1C_1 = 1 \end{aligned}\right\}$$

Therefore, since

$$\lambda_{r_1+r_2+r_3} = \lambda_7 = \lambda_{\{2^{(n-k)}-1\}2^i+i_{\{2^{(n-k)}-1\}}} = \lambda_{2^2+i_1},$$

$$i_1 = 3 \tag{7.34}$$

can be obtained. Therefore, from (7.23),

Accordingly,

$$\left.\begin{aligned} z_0 &= z_7 \\ \\ \\ z_1 &= z_6 \\ z_2 &= z_5 \\ z_3 &= z_4 \end{aligned}\right\} \qquad (7.35)$$

can be obtained. Therefore, from Eqs. (7.35) and Eq. (7.25),

$$x_0 = \sqrt{8}\,(z_0 + z_1 + z_2 + \ldots + z_7) = 2\sqrt{8}\,(z_0 + z_1 + z_2 + z_3) \not\equiv 0$$

$$x_1 = \sqrt{8}\,(z_0 - z_1 + z_2 - z_3 + z_4 - z_5 + z_6 - z_7) \equiv 0$$

$$x_2 = \sqrt{8}\,(z_0 + z_1 - z_2 - z_3 + z_4 + z_5 - z_6 - z_7) \equiv 0$$

$$x_3 = \sqrt{8}\,(z_0 - z_1 - z_2 + z_3 + z_4 - z_5 - z_6 + z_7) = 2\sqrt{8}\,(z_0 - z_1 - z_2 + z_3) \not\equiv 0$$

$$x_4 = \sqrt{8}\,(z_0 + z_1 + z_2 + z_3 - z_4 - z_5 - z_6 - z_7) \equiv 0$$

$$x_5 = \sqrt{8}\,(z_0 - z_1 + z_2 - z_3 - z_4 + z_5 - z_6 + z_7) = 2\sqrt{8}\,(z_0 - z_1 + z_2 - z_3) \not\equiv 0$$

$$x_6 = \sqrt{8}\,(z_0 + z_1 - z_2 - z_3 - z_4 - z_5 + z_6 + z_7) = 2\sqrt{8}\,(z_0 + z_1 - z_2 - z_3) \not\equiv 0$$

$$x_7 = \sqrt{8}\,(z_0 - z_1 - z_2 + z_3 - z_4 + z_5 + z_6 - z_7) \equiv 0$$

can be obtained. Therefore, $x_0 \not\equiv 0$, $x_3 \not\equiv 0$, $x_5 \not\equiv 0$, $x_6 \not\equiv 0$ can be obtained. Therefore, the most efficient codes are

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad (7.36)$$

Example 7.2. The case n = 3, p = 3

From Theorem 4.4 and Theorem 4.6,

$$\left.\begin{aligned} \lambda'_0 &= 6 \\ \lambda'_{r_1} &= 0 \\ \lambda'_{r_1+r_2} &= -2 \\ \lambda'_{r_1+r_2+r_3} &= 0 \end{aligned}\right\} \qquad (7.37)$$

can be obtained. From Eq. (7.27),

$$1 \leq k \leq 3 - 3 + 1 = 1$$

can be obtained. Therefore, in this case, k = 1 can be obtained.

Applying Theorem 7.2 to this case,

$$\left.\begin{aligned} 6 + x_1 \cdot 0 + x_2(-2) + x_3 \cdot 0 = 0 \\ 1 + x_1 + x_2 + x_3 = 2^2 = 4 \end{aligned}\right\} \qquad (7.38)$$

$$\left.\begin{aligned} \therefore \quad x_1 = x_3 = 0 \\ x_3 = 3 \end{aligned}\right\} \qquad (7.39)$$

can be obtained.

Since $n - k = 3 - 1 = 2$ and $k = 1$ hold, $k < n - k$ can be obtained. It is clear that Eq. (7.39) satisfies Eq. (7.20).

From Eq. (7.8)

$$\nu_0 = \lambda'_0 + \lambda'_{2+i_1} + \lambda'_{2^2+i_2} + \lambda'_{3\cdot 2+i_3}$$

can be obtained. Therefore, from Eq. (7.39),

$$\left.\begin{aligned} 2 + i_1 &= 3 \\ 2^2 + i_2 &= 5 \\ 3\cdot 2 + i_3 &= 6 \end{aligned}\right\}$$

Accordingly,

$$i_1 = 1$$

$$i_2 = 1$$

$$i_3 = 0$$

can be obtained. Therefore, from Eq. (7.23),

$$\left.\begin{aligned} z_0 = z_3 = z_5 = z_6 \\ z_1 = z_2 = z_4 = z_7 \end{aligned}\right\} \qquad (7.40)$$

can be obtained.

Therefore, from Eqs. (7.40) and Eq. (7.25),

$$\left.\begin{array}{c} x_0 \not\equiv 0 \\ \\ x_7 \not\equiv 0 \\ \\ x_1 = x_2 = x_3 = x_4 = x_5 = x_6 \equiv 0 \end{array}\right\} \qquad (7.41)$$

can be obtained. Therefore, the most efficient codes of this case are

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad (7.42)$$

8. GENERAL SOLUTION OF $V\Lambda'V^T = 0$

Since

$$z_i = \frac{1}{\sqrt{N}} (1,1,\ldots,1)\zeta_i \tag{8.1}$$

holds from Definition 3.6,

$$\left.\begin{aligned} x_i &= \sqrt{N}\,(z_0,z_1,\ldots,z_{N-1})u_i^{(n)} = 1 \qquad \text{when } u_i^{(n)^T} \in V \\ x_i &= \sqrt{N}\,(z_0,z_1,\ldots,z_{N-1})u_i^{(n)} = 0 \qquad \text{when } u_i^{(n)^T} \notin V \end{aligned}\right\} \tag{8.1'}$$

can be obtained, where

$$Z = U_n \begin{pmatrix} x_0 & & & 0 \\ & x_1 & & \\ & & \ddots & \\ 0 & & & x_{N-1} \end{pmatrix} U_n$$

(cf. Definition 3.7). Therefore,

$$x_0 = x_1 + \ldots + x_{N-1} = m \tag{8.2}$$

can be obtained where m is the greatest possible number of most efficient codes.

Since

$$z_0 = \frac{1}{\sqrt{N}} (1,1,\ldots,1)\zeta_0,$$

$$z_0 = \frac{m}{\sqrt{N}} \tag{8.3}$$

can be obtained.

Now, the discussion from Eq. (7.24) to Eq. (7.26) holds in general. Therefore, letting the number of x_i such that $x_i \equiv 0$ be α,

$$m = N - \alpha \tag{8.4}$$

can be obtained.

Since each z_i for any i $(0 \leq i \leq N - 1)$ can be expressed as a linear combination of $x_0, x_1, \ldots, x_{N-1}$ from Eq. (8.1), "α" elements of $z_0, z_1, \ldots, z_{N-1}$ can be considered the independent variables.

From Eq. (8.4), in order to let m be a maximum, it is necessary to let α be a minimum, that is,

$$\max(m) = N - \min(\alpha) \tag{8.5}$$

Now, let the relation among $z_0, z_1, \ldots, z_{N-1}$ obtained from Eq. (3.27), i.e., $Z\Lambda'Z = 0$ be

$$R_1 \text{ or } R_2 \text{ or } R_3 \text{ or } \ldots \tag{8.6}$$

If the relation in which the number of independent variables among $z_0, z_1, z_2, \ldots, z_{N-1}$ is a minimum is selected among the relations R_1, R_2, R_3, ..., the number is $\max(N - \alpha)$, i.e., $\max(m)$.

Example 8.1. The case $n = 3$, $p = 2$

This case is Example 7.1. Here, the case will be solved by the method developed in this section.

From Eq. (7.29),

$$\left.\begin{aligned} \lambda'_0 &= 3 \\ \lambda'_1 = \lambda'_2 = \lambda'_4 &= 1 \\ \lambda'_3 = \lambda'_5 = \lambda'_6 &= -1 \\ \lambda'_7 &= -3 \end{aligned}\right\}$$

holds. Therefore, from the equation $Z\Lambda'Z = 0$,

$$\left\{\begin{aligned} z_0z_1 &= z_6z_7 && (8.7) \\ z_0z_2 &= z_5z_7 && (8.8) \\ z_0z_3 &= z_4z_7 + z_5z_6 - z_1z_2 && (8.9) \\ z_0z_4 &= z_3z_7 && (8.10) \\ z_0z_5 &= z_2z_7 + z_3z_6 - z_1z_4 && (8.11) \\ z_0z_6 &= z_1z_7 + z_3z_5 - z_2z_4 && (8.12) \end{aligned}\right.$$

$$\left\{\begin{aligned} z_1z_3 &= z_4z_6 && (8.13) \\ z_1z_5 &= z_2z_6 && (8.14) \\ z_2z_3 &= z_4z_5 && (8.15) \end{aligned}\right.$$

$$\begin{cases} 3(z_0^2 - z_7^2) + z_1^2 + z_2^2 + z_4^2 - (z_3^2 + z_5^2 + z_6^2) = 0 & (8.16) \\ 3(z_1^2 - z_6^2) + z_0^2 + z_3^2 + z_5^2 - (z_2^2 + z_4^2 + z_7^2) = 0 & (8.17) \\ 3(z_2^2 - z_5^2) + z_3^2 + z_0^2 + z_6^2 - (z_1^2 + z_7^2 + z_4^2) = 0 & (8.18) \\ 3(z_3^2 - z_4^2) + z_2^2 + z_1^2 + z_7^2 - (z_0^2 + z_6^2 + z_5^2) = 0 & (8.19) \end{cases}$$

can be obtained.

Substituting (8.7), (8.8), (8.10) in (8.9),

$$(1 - \frac{z_7^2}{z_0^2})(z_0z_3 - z_5z_6) = 0 \tag{8.20}$$

can be obtained. Similarly, substituting (8.7), (8.8), (8.10) in (8.11) and (8.12),

$$(1 - \frac{z_7^2}{z_0^2})(z_0z_5 - z_3z_6) = 0 \tag{8.21}$$

$$(1 - \frac{z_7^2}{z_0^2})(z_0z_6 - z_3z_5) = 0 \tag{8.22}$$

respectively can be obtained.

From (8.20), (8.21) and (8.22),

(I) $z_7^2 = z_0^2$

(II)
$$\begin{cases} z_0 z_3 = z_5 z_6 & (8.23) \\ z_0 z_5 = z_3 z_6 & (8.24) \\ z_0 z_6 = z_3 z_5 & (8.25) \end{cases}$$

can be obtained.

From (II),

$$z_0^3 z_3 z_5 z_6 = z_3^2 z_5^2 z_6^2$$

$$\therefore \quad z_3 z_5 z_6 (z_3 z_5 z_6 - z_0^3) = 0$$

can be obtained. Therefore,

(II.1) $z_3 z_5 z_6 = 0$

or

(II.2) $z_3 z_5 z_6 = z_0^3$

can be obtained.

In (II.1), when $z_3 = 0$, from (8.24), (8.25),

$$z_5 = z_6 = 0$$

can be obtained. Similarly whe $z_5 = 0$, $z_3 = z_6 = 0$ can be obtained, and when $z_6 = 0$, $z_3 = z_5 = 0$. Therefore, when (II.1),

$$z_3 = z_5 = z_6 = 0 \tag{8.26}$$

can be obtained. Therefore, from (8.7), (8.8) and (8.9),

$$z_1 = z_2 = z_4 = 0 \tag{8.27}$$

can be obtained. Therefore, from (8.16),

$$z_7^2 = z_0^2$$

can be obtained. Therefore, (II.1) can be reduced to (I).

Therefore, only the cases (I) and (II.2) may be analyzed.

(I) The case $z_7^2 = z_0^2$

$$\therefore \quad z_7 = \pm z_0$$

holds.

(I.1) When $z_7 = z_0$

$$z_1 = z_6 \tag{8.28}$$

$$z_2 = z_5 \tag{8.29}$$

$$z_4 = z_3 \tag{8.30}$$

can be obtained. These relations, i.e., $z_7 = z_0$, (8.28), (8.29), (8.30) clearly satisfy the relation (8.13) to (8.19). Therefore, in this case, the number of independent variables among z_0, z_1, ..., z_7 is 4. Therefore, the greatest possible number, i.e., max(m) = 4 can be obtained.

As in Example 7.1, using the relations $z_7 = z_0$, (8.28), (8.29), (8.30) to

$$x_i = \sqrt{N}\,(z_0, z_1, \ldots, z_7)u_i$$

$$x_0 = 1,\ x_3 = 1,\ x_5 = 1,\ x_6 = 1,\ x_1 = x_2 = x_4 = x_7 = 0$$

can be obtained. Therefore, the most efficient codes are

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

(I.2) $z_7 = -z_0$

From (8.7), (8.8), (8.10),

$$\left.\begin{array}{l} z_1 = -z_6 \\ z_2 = -z_5 \\ z_4 = -z_3 \end{array}\right\} \qquad (8.31)$$

can be obtained. These relations, including $z_7 = -z_0$, clearly satisfy the relations from (8.13) to (8.19). Therefore, in this case, the number of independent variables among $z_0, z_1, \ldots, z_7$ is 4. Therefore, the greatest possible number, i.e.,

$$\max(m) = 4$$

can be obtained.

From $z_7 = -z_0$ and (8.31), similarly

$$x_1 = x_2 = x_4 = x_7 = 1$$

$$x_0 = x_3 = x_5 = x_6 = 0$$

can be obtained. Therefore, the most efficient codes are

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

(II.2) The case $z_3 z_5 z_6 = z_0^3$

From $z_3 z_5 z_6 = z_0^3$ and (8.23),

$$z_0 z_3^3 = z_0^3$$

$$\therefore \quad z_3^3 = z_0^2 \qquad (\because \quad z_0 = \frac{m}{\sqrt{N}} > 0 \quad (\text{cf. Eq. } (8.3))) \tag{8.32}$$

can be obtained. Similarly (8.24) and (8.25),

$$z_3^2 = z_5^2 = z_6^2 = z_0^2 \tag{8.33}$$

can be obtained.

On the other hand, from $z_3 z_5 z_6 = z_0^3 > 0$ ($\because$ $z_0 = \frac{m}{\sqrt{N}} > 0$)

$$\left.\begin{matrix} z_3 > 0 \\ z_5 > 0 \\ z_6 > 0 \end{matrix}\right\} \quad \text{or} \quad \left.\begin{matrix} z_3 > 0 \\ z_5 < 0 \\ z_6 < 0 \end{matrix}\right\} \quad \text{or} \quad \left.\begin{matrix} z_3 < 0 \\ z_5 > 0 \\ z_6 < 0 \end{matrix}\right\} \quad \text{or} \quad \left.\begin{matrix} z_3 < 0 \\ z_5 < 0 \\ z_6 > 0 \end{matrix}\right\}$$

must hold. Therefore,

$$z_3 = z_5 = z_6 = z_0$$

or

$$z_3 = -z_5 = z_6 = z_0$$

or

$$-z_3 = z_5 = -z_6 = z_0$$

or

$$-z_3 = -z_5 = z_6 = z_0$$

can be obtained.

Therefore, from (8.7), (8.8), (8.9) and the above relations,

$$z_1 = z_2 = z_4 = z_7, \; z_3 = z_5 = z_6 = z_0$$

or

$$z_1 = z_2 = -z_4 = -z_7, \; z_3 = -z_5 = -z_6 = z_0$$

or

$$-z_1 = z_2 = -z_4 = z_7, \; -z_3 = z_5 = -z_6 = z_0$$

or

$$z_1 = -z_2 = -z_4 = z_7, \; -z_3 = -z_5 = z_6 = z_0$$

can be obtained. These relations also satisfy the relations from (8.13) to (8.19). Therefore, in these cases, the number of independent variables among $z_0, z_1, \ldots, z_7$ is 2. Therefore, the greatest possible number, i.e.,

$$\max(m) = 2$$

can be obtained.

Calculating $x_i = \sqrt{N}\,(z_0, z_1, \ldots, z_N)u_i$ by using these relations, the following results can be obtained:

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Finally, $\max(m) = 4$, the greatest possible number, that is (I.1) and (I.2), can be obtained.

9. GENERAL SOLUTION OF $V\Lambda'V^T = 0$ IN APPLICATION OF BOOLEAN ALGEBRA

A necessary and sufficient condition that $V\Lambda'V^T = 0$ is that

$$x_i x_j h_{i\oplus j} = 0 \tag{9.1}$$

when $i \neq j$ $(0 \leq i, j \leq 2^n - 1)$, and that $x_i^2 h_0' = 0$ for $0 \leq i \leq 2^n - 1$. Equation (9.1) follows from Eq. (7.24), and $x_i^2 h_0' = 0$ because $h_0' = 0$.

Since $x_i = 1$ or 0 holds for any i $(0 \leq i \leq 2^n - 1)$ from Eq. (8.1'), x_i can be considered as a variable of a Boolean function.

In order to satisfy Eq. (9.1), when $h_{i\oplus j} = 1$, $x_i x_j = 0$ must hold, but when $h_{i\oplus j} = 0$, the value of $x_i x_j$ may be arbitrary.

Therefore, when $h_{i\oplus j} = 1$,

$$x_i x_j = 0 \tag{9.2}$$

$$\therefore \quad y_i \vee y_j = 1 \tag{9.3}$$

must hold for any $i \neq j$ $(0 \leq i, j \leq 2^n - 1)$, where y_i is a negation of x_i, i.e.,

$$\left.\begin{aligned} y_i &= x_i' \\ y_j &= x_j' \end{aligned}\right\} \tag{9.4}$$

Therefore,

$$\prod_{\substack{0\leq i,j\leq 2^n-1 \\ i\neq j \\ h_{i\oplus j}=1}} (y_i \vee y_j) = 1 \tag{9 5}$$

must hold. Therefore, after the expansion of Eq. (9.5), choose the term whose number of variables (y_i's) is minimal.

Now, suppose that the term is

$$y_{i_1} y_{i_2} \cdots y_{i_\ell} \tag{9.6}$$

Then if

$$y_{i_1} y_{i_2} \cdots y_{i_\ell} = 1 \tag{9.7}$$

holds,

$$y_{i_1} = y_{i_2} = \ldots = y_{i_\ell} = 1 \tag{9.8}$$

can be obtained. Therefore, from Eq. (9.4) and Eq. (9.8),

$$x_{i_1} = x_{i_2} = \ldots = x_{i_\ell} = 0 \tag{9.9}$$

can be obtained. This means that if $x_{i_1} = x_{i_2} = \ldots = x_{i_\ell} = 0$,

$$V\Lambda' V^T = 0$$

can be obtained, where ℓ is the minimum number of Boolean variables among terms in the expansion of Eq. (9.5) whose Boolean variables are equal to zero.

Therefore, put $x_i = 1$ for any i ($0 \leq i \leq 2^n - 1$), where

$$i \neq i_1,\ i \neq i_2,\ \ldots,\ i \neq i_\ell$$

Then, the greatest possible number of most efficient codes is

$$(N - \ell) \tag{9.10}$$

and the most efficient codes consist of the binary codes corresponding to any i $(0 \leq i \leq 2^n - 1)$ for $i \neq i_1$, $i \neq i_2$, ..., $i \neq i_\ell$.

Remark 9.1. Without loss of generality, $u_0^{(n)} \in V$ can be assumed. Therefore, $x_0 = 1$ can be assumed.

Example 9.1. The case $n = 3$, $p = 2$

From Example 3.3,

$$h_0' = 0,\ h_1 = h_2 = h_4 = 1,\ h_3 = h_5 = h_6 = h_7 = 0$$

can be obtained. Therefore, from Eq. (9.2)

$$\left.\begin{aligned} x_0x_1 &= 0 \\ x_0x_2 &= 0 \\ x_0x_4 &= 0 \\ x_1x_3 &= 0 \\ x_1x_5 &= 0 \\ x_2x_3 &= 0 \\ x_2x_6 &= 0 \\ x_3x_7 &= 0 \\ x_4x_5 &= 0 \\ x_4x_6 &= 0 \\ x_5x_7 &= 0 \\ x_6x_7 &= 0 \end{aligned}\right\} \qquad (9.11)$$

can be obtained. From Remark 9.1,

$$x_0 = 1$$

holds without loss of generality. Therefore, from Eq. (9.5),

$$y_1y_2y_4(y_1 \vee y_3)(y_1 \vee y_5)(y_2 \vee y_3)(y_2 \vee y_6)(y_3 \vee y_7) \cdot (y_4 \vee y_5)(y_4 \vee y_6)(y_5 \vee y_7)(y_6 \vee y_7) = 1 \tag{9.12}$$

can be obtained. Therefore,

$$\begin{aligned} \text{Eq. } (9.12) &= y_1y_2y_4(y_1 \vee y_3y_5)(y_2 \vee y_3y_6)(y_3 \vee y_7)(y_4 \vee y_5y_6)(y_5y_6 \vee y_7) \\ &= y_1y_2y_4(1 \vee y_3y_5)(1 \vee y_3y_6)(y_3 \vee y_7)(1 \vee y_5y_6)(y_5y_6 \vee y_7) \\ &= y_1y_2y_4(y_3 \vee y_7)(y_5y_6 \vee y_7) \\ &= y_1y_2y_4(y_3y_5y_6 \vee y_7) \\ &= y_1y_2y_4y_7 \vee y_1y_2y_3y_4y_5y_6 \qquad (9.13) \end{aligned}$$

The term of the right-hand side of Eq. (9.13) whose number of variables is minimal is

$$y_1y_2y_4y_7$$

Therefore, the greatest possible number of most efficient codes is $2^3 - 4 = 4$. Therefore,

$$y_1y_2y_4y_7 = 1$$

can be obtained. Therefore,

$$x_1 = x_2 = x_4 = x_7 = 0$$

Accordingly,

$$x_0 = x_3 = x_5 = x_6 = 1$$

can be obtained. Therefore, the most efficient codes are

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

10. CONCLUSION

Most efficient codes were found in principle by the methods discussed above.

Now, define m_G, m_C, m_O as follows:

m_G: the number of most efficient group codes

m_C: the number of most efficient codes under Condition 6.1 and Condition 6.2

m_O: the number of most efficient codes in general

From the description of Section 7 and Remark 7.3,

$$2 \leq m_G \leq m_C \leq m_O \leq 2^{n-p+1} \qquad (10.1)$$

can be obtained.

As a future problem, do there exist most efficient codes under Condition 6.1 and Condition 6.2 such that $m_C > m_G$? Another problem is to obtain an elegant method of solution for general most efficient codes such that $m_O > m_C$.

This paper has presented a new conclusion, that the most efficient codes problem under Condition 6.1 and Condition 6.2 including group codes has been solved completely.

N